Good identity management helps academic institutions avoid financial loss, inefficiency in business processes and legal liability for mismanagement of personal data.

The JISC Identity Management Toolkit is designed to support ICT directors, managers and staff in universities and colleges.
Table of Contents

Toolkit Contents........................................................................................................................................6
About the Complete Printable Version of the Identity Toolkit.............................................................7
   Terms of Use........................................................................................................................................7
   Legal and Regulatory compliance........................................................................................................7
   Navigating the complete printable Toolkit............................................................................................7
   Updates to the Toolkit............................................................................................................................7
   Acknowledgements..............................................................................................................................7
   Disclaimer............................................................................................................................................9

1 Introduction........................................................................................................................................10
   Executive Summary..............................................................................................................................10
   Section contents................................................................................................................................10
   1.1 What is identity ............................................................................................................................10
   1.2 What is identity management (IdM) and why do we need to think about it?...............................10
   1.3 IdM definition................................................................................................................................11
   1.4 Identity management in further & higher education (FHE)............................................................13
   1.5 What is the Identity Management Toolkit and why is it needed?....................................................15
      Toolkit Versions..............................................................................................................................16
      Note...............................................................................................................................................16

2 Identity Management Governance and Policies............................................................................17
   2.1 Introduction....................................................................................................................................17
      Executive summary ............................................................................................................................17
      Section contents................................................................................................................................17
   2.2 Governance structure overview....................................................................................................17
   2.3 Provision of IdM services................................................................................................................19
      2.3.1 IdM governance board...........................................................................................................19
      2.3.2 IdM director (program manager)...........................................................................................19
      2.3.3 Technical oversight.................................................................................................................19
      2.3.4 IdM service department..........................................................................................................19
      2.3.5 Advice centres.......................................................................................................................19
      2.3.6 Other governance bodies.......................................................................................................20
   2.4 Consumption of IdM services.........................................................................................................20
      2.4.1 IdM system...............................................................................................................................20
      2.4.2 Organisational units................................................................................................................20
      2.4.3 End users................................................................................................................................20
      2.4.4 Other systems..........................................................................................................................21
      2.4.5 Contractors, partners, other third parties..............................................................................21
   2.5 Identity lifecycle and policy areas....................................................................................................21

3 Identity Management Systems, Components and Functions......................................................26
   3.1 Introduction ....................................................................................................................................26
      Executive Summary............................................................................................................................26
      Section contents................................................................................................................................26
   3.2 Core IdM system components.........................................................................................................26
      3.2.1 Identity repository and lifecycle management...........................................................................27
      3.2.2 Authentication service.............................................................................................................27
      3.2.3 Authorisation service................................................................................................................28
      3.2.4 Directory service.......................................................................................................................28
      3.2.5 Groups service..........................................................................................................................29
      3.2.6 Asset repository.......................................................................................................................29
      3.2.7 Overview diagram...................................................................................................................30
      3.2.8 Consolidated overview with access control............................................................................31
   3.3 Federated access..............................................................................................................................32
      3.3.1 Shibboleth..................................................................................................................................32
      3.3.2 Other considerations.................................................................................................................34
   3.4 Provisioning in more detail...............................................................................................................34
      3.4.1 Synchronisation.......................................................................................................................36

4 Defining Institutional Requirements: ................................................................................................38
   4.1 Introduction....................................................................................................................................38
Toolkit Contents

1. Introduction to Identity Management
Start here! Defines basic terms and concepts of Identity Management used or assumed elsewhere. Should be read by anyone using the Toolkit.

2. Identity Management Governance and Policies
Describes the roles, structures and policies required for Identity Management and how they relate to Identity Management systems and processes. Useful for Chief Information Officers or Directors responsible for IT, and staff who need to draft or apply institutional policies.

3. Identity Management Systems, Components and Functions
The technical components and functions of Identity Management systems in an academic institution. Good background reading for IT service managers and staff, and anyone discussing Identity Management with potential system suppliers.

4. Defining Institutional Requirements
Functional requirements for each component of an Identity Management system, which may be useful in defining the objectives of an in-house implementation project or in detailed specifications to suppliers.

5. Discovering and Auditing Current Institutional Identity Management
A detailed guide to finding out the state of Identity Management in an institution with a comprehensive audit (based on work of the JISC Identity Project which developed and tested IdM audits in several universities).

6. Gap Analysis
Explains how to establish the current and desired states of affairs for Identity Management, gives a list of common gaps in FHE institutions, and suggests ways for developing a strategy.

7. An Institutional Roadmap for Identity Management
Producing an overall roadmap or programme plan. Prioritising major deliverables and milestones by achievability, cost and institutional impact.

8. Ensuring Continuity of High Quality IdM
Keeping a high profile for IdM in the institution, understanding how to apply IdM principles to new initiatives in the institution, and ensuring that members of the institution know about the local and global aspects of IdM as they apply to their role within the institution.

9. Designing and Managing an Identity Management Project
Project management issues particular to implementing Identity Management, including key institutional benefits of improved Identity Management for use in an institutional business case.

10. Selecting Supplier Solutions
Where commercial procurement of systems or components is required, this section aims to help understand the IdM system solutions available, produce procurement criteria, and construct tender documents.

Identity Management Glossary
Not an exhaustive list but contains terms and abbreviations used in IdM, and in other sections of the Toolkit, and their meanings in an IdM context.
About the Complete Printable Version of the Identity Toolkit

Terms of Use
The Identity Management Toolkit is the copyright of JISC and the contributing authors. It is made available under a Creative Commons UK Attribution, Non-commercial, Share-Alike license. To discuss waivers or potential commercial use, please contact jiscinfolnet@northumbria.ac.uk.

In plain English, the project to produce the Toolkit has been funded on behalf of the United Kingdom Further & Higher Education community (member colleges and universities of JISC) and all non-commercial users, including accredited universities and colleges worldwide, are encouraged to make use of material included in the Toolkit. If you wish to use or adapt text or graphics from the Toolkit in documents produced for use in your educational institution you may do so freely. Please credit “the JISC Identity Management Toolkit” and quote the URL “www.Identity-Project.org” in all derived material.

If you are intending to publish material derived from the Toolkit outside your own institution it should be covered by a comparable Creative Commons license; but we do not need you to ask us for a waiver if you intend to use such material only with staff and students of your own academic institution. We would be very pleased to hear, though (please email jiscinfolnet@northumbria.ac.uk) about any use of material in the Toolkit.

Cover graphics used in printed/printable versions of the Toolkit are copyright HEFCE on behalf of JISC and used under a Creative Commons UK Non-commercial, Attribution, Non-derivative licence; which means that these should not be re-used in material other than the Toolkit without permission from JISC.

Where possible, graphics such as diagrams used in the Toolkit have also been included (in the online version only) in ‘source’ formats (such as Microsoft Visio™ files), and users are free to use and adapt these for use in their own institutional briefings and other documents. Similarly, users may use text copied from either the printable or online versions. Please credit “the JISC Identity Management Toolkit” and quote the URL “www.Identity-Project.org” as the source from which your own diagram or text was derived.

Legal and Regulatory compliance
Information about legal and regulatory requirements in all sections of the Toolkit is considered accurate by the authors at the time of writing (August 2009 to February 2010), and have been checked again on revision (February to August 2012). To ensure compliance with current rules and legislation, up to date independent and qualified advice should be sought to inform any decisions by your organisation.

Navigating the complete printable Toolkit
As far as the media allows, the contents of the complete printable and online versions of the Toolkit are identical, including numbering of main sections and subsections. The Contents and Summary briefly outlines the purpose and intended readership of each main section and the entire content is indexed by page number at the start of the document. As far as possible references by URL to external documents and resources in a section are repeated under the heading “Resources” at the end of the document, with the URL in human-readable form. The Toolkit also contains a Glossary of terms used, as an appendix.

Some cross-references to internal resources (contained in the online version of the Toolkit) will be to the online section to which an item is attached.

Updates to the Toolkit
After initial publication (August 2012) of the Toolkit updates and corrections may be made to the online version of the Toolkit. Unfortunately, there is no facility for incorporating such changes into the PDF versions of the Toolkit.

Acknowledgements
The original Identity Management Toolkit was written, tested, edited and produced by a team from the
partner institutions in the project:

- Kidderminster College
- The University of Bristol
- Cardiff University
- The London School of Economics & Political Science

The project was funded by JISC with contributions from partners and undertaken between January 2009 and June 2010.

Updates to the toolkit were funded by JISC between January and August 2012, with contributions from some members of the original team and project board, named in bold type in the lists below.

Contributing members of the **Project Team** were:

- Ralph Ballon
- Ed Beddows
- Gary Brown
- Masha Garibyan
- Julia Lloyd
- Simon McLeish
- Andrew Morris
- John Paschoud *Project Manager*
- Paul Rock
- Phil Smart
- Rhys Smith
- Luke Taylor
- Becky Williams

The external reviewer for the original version was Paul Salotti.

Judy Redfearn and Greg Clemett of JISC Communications provided valuable assistance with the design and production of cover graphics and publicity material, used for both versions of the Toolkit.

Members of the **Project Board**, and the organisations they represented, were:

- Christopher Brown (JISC Innovation) *JISC Programme Manager*
- Noel Davis (JISC Regional Support Centres)
- Adrian Ellison (London School of Economics)
- Stephan Freeman (ISAF)
- Ian Griffiths (UCISA)
- David Harrison (Cardiff University)
- Graham Mason (Kidderminster College)
- Tim Phillips (University of Bristol) *Project Board Chair*
- David Speake (RUGIT)
- Andrew Stewart (JISC infoNet)
Disclaimer

The information contained in all published versions of the Identity Management Toolkit (the Toolkit) is for general information purposes only. The information is provided by JISC and the partner institutions involved in the project (the Project) and while we endeavour to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the Toolkit or the information, products, services, or related graphics contained in the Toolkit for any purpose. Any reliance you place on such information is therefore strictly at your own risk.

In no event will we be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of the Toolkit.

Through links provided in online and printable versions of the Toolkit you are able to access other websites which are not under the control of the Project. We have no control over the nature, content and availability of those sites. The inclusion of any links does not necessarily imply a recommendation or endorse the views expressed within them.

Every effort is made to keep all versions of the Toolkit available and functional. However, the Project takes no responsibility for, and will not be liable for, any version of the Toolkit being temporarily unavailable due to technical issues beyond our control.
1 Introduction

Executive Summary

It is recommended that all users of the Toolkit read this short section which defines basic terms and concepts of Identity Management used or assumed elsewhere.

Section contents

• 1.1 What is identity?: Defines what is meant by identity.
• 1.2 What is identity management (IdM) and why do we need to think about it?: Describes Identity Management and the reasons it is important.
• 1.3 IdM definition: Defines Identity Management, and describes the identity lifecycle.
• 1.4 Identity management in further & higher education (FHE): Describes the special requirements for Identity Management in the FHE sector.
• 1.5 What is the Identity Management Toolkit and why is it needed?: Describes the Toolkit and its purpose.

1.1 What is identity

One definition of identity (Oxford English Dictionary) is:

The sameness of a person or thing at all times or in all circumstances; the condition or fact that a person or thing is itself and not something else.

We are given a name at (or shortly after) birth. Within a small community a name may be sufficient to refer to a specific person unambiguously. However, beyond that community, a name will often not be unique, or there may be no means to verify that someone is who they say they are. Knowing that someone is who they say they are is the first basis of trust, entitlement and accountability.

All modern societies have found it necessary to provide means by which identities may be independently verified, e.g. birth certificates and passports, and proof of identity is a pre-requisite for many activities, e.g. opening a bank account.

The above definition should not be taken to mean that identities do not change. In fact, over time, many attributes relating to an identity will change e.g. when someone adopts the surname of their spouse, and coping with such changes is one of the challenges of identity management.

1.2 What is identity management (IdM) and why do we need to think about it?

Identity management, in a general sense, includes all the processes and systems that allow the creation, retrieval, update, verification and destruction of identities and information relating to identities including any rights / authority granted to the identities. It is important to note that identities have been, and continue to be, managed using paper-based systems operated by people. In addition, many IT based identity management systems are used to create artifacts (e.g. identity cards) which may be subject to visual checks and/or machine-based verification.

Identity management in computing involves the mapping of real world identities to electronic identities and ensures appropriate use of IT systems. It is important because the use of IT systems has become pervasive in many aspects of life. IT systems may be, and are, misused to breach confidentiality, perpetrate fraud and disrupt critical activities. Furthermore, legislation has been introduced, including the Data Protection Act 1998, the Copyright, Designs and Patent Act 1988, The Regulation of Investigatory Powers Act (RIPA) 2000 and the Computer Misuse Act 1990, that place legal requirements on businesses to protect personal privacy and to ensure the confidentiality and security of their information. Holders of personal data must not only be registered under the Data Protection Act, but also take adequate steps to protect that data from unauthorised access.

Aside from security concerns, consistent and accurate use of identities across IT systems increases
organisational efficiency and flexibility, and improves user experience (through personalisation\(^1\) and customisation\(^2\)), leading to reduced costs and competitive advantage.

It is worth noting that much of the success of Web 2.0 / social web, has been due to the ability of individuals to organise themselves. Leveraging an IdM system to allow self-organisation has the potential to facilitate many of the informal processes that are important to the ways that organisations operate.

### 1.3 IdM definition

Wikipedia defines identity management as:

> In information systems, identity management is the management of the identity life cycle of entities (subjects or objects). An identity management system:

1. Establishes the identity
   1. Links a name (or number) with the subject or object;
   2. Re-establishes the identity (i.e. links a new or additional name, or number, with the subject or object);
2. Describes the identity:
   1. Optionally assigns one or more attributes applicable to the particular subject or object to the identity;
   2. Re-describes the identity (i.e. changes one or more attributes applicable to the particular subject or object);
3. Follows identity activity:
   1. Record and/or provide access to logs of identity activity
   2. Optionally auto-analyze behaviour patterns of the identity
4. Destroys the identity

The diagram overleaf illustrates the identity life cycle and the importance of an IdM system in integrating identities with business systems. The diagram is discussed further in the Governance section of the Toolkit.

In practice, IdM is concerned with:

- managing identity information including:
  - how and where information is stored - for all types of identities including atypical users\(^3\)
  - how data is classified e.g. with respect to privacy / sensitivity
  - how information is transported
  - how information is disposed of
  - who can view and / or change information
  - prior id discovery i.e. matching, where appropriate, a new identity with an existing identity e.g. where a former student becomes a member of staff
- integration
  - which identities and what information about them is made available to which systems
  - accuracy and timeliness of information throughout systems e.g. to reflect the identity life cycle
  - extension of security model from the IdM system to other systems
- security and access control
  - credential types
  - transport protocols
  - federated access i.e. enabling users to access external resources and enabling external users to access local resources

---

1. Personalisation is the targeting of services to individuals based on their identity attributes. It allows the organisation to push relevant and appropriate services e.g. a Portal may show department specific information - the information may not be sensitive or require access control but it does not make sense to present irrelevant information for many departments
2. Customisation allows individuals to determine some of their own attributes e.g. subscription to a subject specific news service. In this case the individual pulls services they deem to be relevant.
3. Atypical users may include a wide range of users who do not fall into traditional staff / student categories. The diagram in the next section gives an overview of different associations an individual may have with an FHE organisation.
• compliance and governance
  • audit trails i.e. who viewed / changed information
  • prevention of misuse
  • policy for all of the above which complies with current legislation
  • audit and enforcement of policy

Naturally organisations have a sense of ownership over identities they manage and are most concerned with their own activities and responsibilities, however, from the perspective of an individual this is not always a satisfactory approach. An individual often has affiliations with other organisations leading to multiple identities.
across a range of systems. There are a number of initiatives aimed at giving individuals more control over their identity e.g. OpenId\(^4\) and this is an area where FHE organisations need to be engaged in order to meet user expectations and to facilitate collaboration.

All organisations operate systems which would fall under the definition above, however, in general, most organisations have sub-optimal and ad hoc systems which have evolved rather than been designed or planned. In this document an identity management system (IdM system) refers to a system which:

1. is secure and allows appropriate restrictions on the use of IT systems and other facilities
2. complies with legislation
3. has been designed and sized to manage all identities relevant to an organisation, including external identities
4. supports organisational processes in an integrated, timely, flexible and efficient manner

or, in summary, is fit-for-purpose.

### 1.4 Identity management in further & higher education (FHE)

FHE organisations have the same security and legal obligations as other organisations. As in any sector FHE organisations also have many similarities:

- large intakes of new identities at least once per year
- a strong ethos of openness and collaboration with academics and students collaborating on projects and visiting partner organisations
- partnerships within HE and with businesses and the local community
- medical schools have close links with the NHS
- continuing relationship with alumni
- IT systems developed for and/or targeted at the sector e.g. Student record systems, virtual learning environments (VLEs) and Library systems

There are benefits to the sector in adopting common standards-based approaches:

- organisations may choose systems from different vendors without being locked in
- the sector can influence the development of standards
- organisations can share relevant experiences
- funding organisations are more likely to contribute to infrastructure if it will be used throughout the sector e.g. JISC and JANET support and operate the UK Access Management Federation for Education and Research. Federation members may access resources hosted by other federation members using Shibboleth. Members only need to authenticate at their home organisation using their usual credentials.

The complexity of FHE organisations is summarised in the diagram overleaf.

Key challenges include:

- the number of individuals involved in the organisation i.e. thousands to tens of thousands
- managing the many different membership types
- providing a wide range of systems and facilities to support the wide range of activities undertaken
- controlling, as appropriate, access to systems and facilities
- maintaining reliable, accurate and timely data across systems
- overlapping responsibilities and systems e.g. students may be associated with a course, department, school and faculty which may operate local systems
- allowing external users access to systems and facilities
- allowing users to access external systems and facilities
- providing a coherent user experience, particularly when users may have more than one role i.e. a member of staff may also be an alumnus enrolled on a masters course whilst applying to do a PhD on completion of their current studies.
- different membership types are generally the responsibility of different departments and are managed in different systems
- access to systems is often managed, by different teams, in system-specific ways

\(^4\) [http://openid.net/](http://openid.net/)
data captured to support one activity or system is not available to other systems or is inadequate for use in another system.

IdM can help meet these challenges, and, in so doing, support the core activities of FHE organisations by providing a coherent model of the organisation and its members, activities, facilities and systems, which can be managed in an efficient and consistent way. In particular, taking a wide view of IdM allows organisations to take what are generally considered to be a series of separate processes and re-engineer them as variants of a single process e.g. requests for specific levels of access to individual systems are generally handled by
separate teams responsible for the different systems. Implementing a central IdM system would enable all requests to be made using a single process which may select different rules depending on:

- who is making a request
- on whose behalf the request is being made
- the system to which access is being requested

For example, a request made by a head of department may be accepted without further intervention whereas other requests may appear in a task list for the team responsible for the system, or in a task list for the head of department.

Such a process would provide organisation wide metrics on how often requests are made and how quickly they are dealt with.

### 1.5 What is the Identity Management Toolkit and why is it needed?

The Toolkit defines:

- identity management (IdM)
- all the key IdM components
- policies required to operate an IdM system

It provides a detailed requirements specification for each component and provides a process, and tools, to help:

- audit current IdM policies, processes and systems
- perform IdM gap analysis
- produce a business case for IdM
- produce an IdM roadmap
- procure an IdM system

The JISC Identity Project found that there was little consensus, even within organisations, on what IdM is, along with a number of common gaps in IdM practice. The Toolkit is needed to:

- set IdM in context
- provide a clear definition of what IdM is
- define clear benefits for improving IdM practice in FHE
- provide guidance on how to approach IdM from policy and technical perspectives

Implementing an IdM system is a major undertaking. It involves much more than installing a new IT system. It will involve many changes to existing systems and processes, affecting many people. In the short term it will cost time, money and effort. Without being able to make a business case or being able to develop a clear roadmap it is unlikely that a project will gain the high-level support required to secure adequate funding and the institutional acceptance required for success.

The FHE sector as a whole can benefit from improved IdM practice in individual organisations as it helps to overcome technical barriers to collaboration between organisations and facilitates sector wide initiatives. It also has the potential to provide effective life long learning for students.

The material in the Toolkit, particularly in the Audit section, is intended to contain material applicable to as wide a range of organisations from the FHE sector as possible. This means that it is important to decide which material is relevant to your particular institution or organisation before making use of it. The intention is also to be advisory rather than prescriptive, and the Toolkit should be read in this light: the material should be adapted to fit the local requirements and culture, not necessarily used precisely as it appears here. The Toolkit should be applied in a way which is tailored to the organisation’s size and complexity, recognising the environment within which it operates.

### Toolkit Versions

The Identity Management Toolkit exists in five versions, as revised in 2012, all available for download or browsing from www.Identity-Project.org. These are:
• The online Toolkit, version 2. This version consists of web pages and includes downloadable resources, such as source files to enable diagrams to be re-used and adapted. While the main content of this will remain essentially static, there is also an associated blog which will be used to post additional material from time to time.
• The complete printable Toolkit, version 2. This is a PDF document consisting of the full textual contents of the online Toolkit, without the associated downloadable resources.
• The concise printable Toolkit, version 2. This is a more accessible PDF document, intended as an introduction to the complete Toolkit, and includes some content and summaries of the remainder.
• The older online Toolkit, version 1. This is still accessible, but is now replaced by version 2.
• The printable version of the older online Toolkit, derived from the online content, also available as a PDF from www.Identity-Project.org.

This document is the complete printable Toolkit, version 2.

Note
Throughout the Toolkit, the abbreviation FHE is used for “the further and higher education and skills sector”, and FHEI for “FHE institution”.

16 of 123
2 Identity Management Governance and Policies

2.1 Introduction

Executive summary
This section describes the general roles, structures and policy areas required to operate Identity Management safely and effectively in an education institution; and how they relate to the technical elements of Identity management systems and processes.

Section contents

• 2.1 Introduction: Explains the need for governance and policies.
• 2.2 Governance structure overview: Describes a generalised description of the roles and relationships needed to operate an effective IdM system.
• 2.3 Provision of IdM services: Describes the roles of the different groups of individuals involved in the provision of IdM services.
• 2.4 Consumption of IdM services: Describes the ways in which IdM services are used and the responsibilities of those who use them.
• 2.5 Identity lifecycle and policy areas: Describes how the identity lifecycle relates to the different areas of IdM policy.

The law places obligations on organisations which collect personal data and operate computer and network facilities. It also grants rights to individuals whose personal data has been collected and/or who use computer and network facilities. An IdM system and the way it is operated must, therefore, comply with all relevant legislation.

The recommendations from the UCISA Information Security Toolkit, many of which are designed to comply with applicable legislation, also directly apply to IdM systems. Note, however, an effective IdM system will also make it easier to adopt those recommendations and provide evidence of compliance by, for example:

• controlling the life cycle of user accounts and reducing the need for local accounts
• enforcing consistent policies
• enforcing transparent business rules and workflow including pre-requisites such as training or dual sign-off
• enforcing credential management policies
• making clear the lines of authority and accountability
• recording the granting and revocation of privileges
• centralising access control decisions
• ensuring accurate and timely data
• logging usage
• central reporting
• facilitating data retrieval for subject access requests

However, effective identity management requires much more than an IT-based IdM system. Such a system should simply reflect policies which have been developed by the appropriate governance structure and facilitate compliance. In particular, information which has been exported from an IdM system, either electronically or on paper or other physical media is prone to loss, misuse and theft. Policies must cover handling of data once it leaves the IdM system.

2.2 Governance structure overview

The diagram overleaf outlines the general roles and relationships required to operate an effective IdM system. How these are mapped onto actual jobs and individuals/groups will of course vary with the differences in size, traditions and existing structures of FHE institutions, and some roles may be combined.

Elements of the diagram are discussed in the following sections, however, it is worth emphasising the need for continuous awareness of other initiatives within the institution. In recent years uncertainty about FHE funding, larger student loans and new regulatory requirements have prompted many FHEIs to embark on significant organisational change to both support and academic services, in order to increase efficiency and to allow greater focus on student experience. The scale and nature of the changes has made many organisations review and enhance their existing programme/project management infrastructure/methodologies including looking at new frameworks and tools e.g. enterprise architecture and service oriented architecture.

It is important that the IdM project team and sponsors are aware of ongoing change in the institution and proactively engage with other projects to raise awareness of what IdM is and ensure that IdM is taken into account. For example, projects which involve new systems and/or business process improvement, including formalising roles and restructuring departments will also have requirements around access and privilege management which could benefit from workflow available in an IdM system. While each institution will have its own process for managing and co-ordinating change, it is recommended that consideration of IdM be made a formal part of any change process.

Understanding the relative importance to senior management of new systems and processes, and their likely timelines may influence the priorities/phasing for the IdM project e.g. if a home grown personnel system is
scheduled for replacement in two years time, it may be appropriate to focus on other areas, or it could be a
prompt to migrate existing point-to-point integrations between the personnel system and other systems, to
facilitate its replacement.

2.3 Provision of IdM services

2.3.1 IdM governance board

For identity management to be effective it must have support from the highest levels of the organisation as
well as the main stakeholders. A representative high level board with decision making powers should
oversee all aspects of IdM practice and be accountable for that practice across the organisation, ensuring
consistent and effective practice. Most board members will not be IdM experts but will be able to draw on
expert knowledge. The board should meet on a regular basis. All requests, decisions and policies should
be transparent and documented. The board should ensure that policies are reviewed on a regular basis and that
IdM practice is audited to ensure compliance with the law and the wider goals of the organisation. For FHE
institutions that have an individual in the role of Chief Information Officer (CIO), it will be appropriate for the
CIO either to assume the role of Chair of the board, or to be the senior staff member reporting to it.

2.3.2 IdM director (program manager)

IdM operations should be headed by a senior member of staff with relevant IdM experience. The IdM director
would be responsible for day to day operations and would report to the IdM governance board. The director
would be expected to keep abreast of identity management risks and issues, and, in particular, their potential
impact on the organisation and the higher education sector in general. In smaller FHE institutions this may
be the CIO; in larger ones this role may report to the CIO.

2.3.3 Technical oversight

Implementation of an IdM system will require integration with many systems and involve many systems
teams. It is important that detailed technical options are agreed and subject to appropriate scrutiny by, for
example, an ICT board, which has responsibility for overseeing technical infrastructure.

2.3.4 IdM service department

Technical staff will be required to maintain and support the IdM system and users of the system. Activities will
include:

• installation, configuration, integration, testing, patching and upgrades
• training, guidance and support for end users and other technical staff
• monitoring and troubleshooting
• reporting

Staff in this department will have an important role in spreading IdM competence and ensuring compliance.
They should have clear guidance on how and when to escalate issues to the IdM director, who, in turn, can
resolve issues or escalate issues to the IdM governance board.

2.3.5 Advice centres

Most organisations will already have structures and policies to deal with data protection and security issues.
With the development of an IdM system it is important to clearly set out roles and responsibilities and to
ensure that experts in the different areas work together and are able to obtain appropriate legal advice,
particularly when legislation changes, new legislation is introduced or legal precedents are set.

Internal and external auditing services should be available which are independent of those operating the IdM
system.
2.3.6 Other governance bodies

Due to the impact of IdM on all areas of the organisation it would be desirable to have representation on other governance bodies for the institution, and perhaps for those bodies to nominate members of an IdM governance board. The names, structures and memberships of such bodies vary widely across FHE institutions and so the Toolkit will not suggest examples.

2.4 Consumption of IdM services

Ultimately the perceived success or otherwise of an IdM system will largely be judged by those who have to use it directly or interact with systems which depend on it. The actual success also depends on how effectively people use the system which, in turn, will depend on appropriate configuration, effective training and support, awareness of responsibilities, and the management and cultural factors which lead to responsibilities being taken seriously and acted on at all times.

2.4.1 IdM system

All data held within the IdM system should be classified for privacy/security reasons and the purposes for which data was collected, and may therefore be used, clearly documented. One security classification system is:

<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public (P)</td>
<td>Visible to anyone</td>
</tr>
<tr>
<td>Open (O)</td>
<td>Visible to any authenticated member of the organisation</td>
</tr>
<tr>
<td>Confidential (C)</td>
<td>Visible to some authenticated members of the University</td>
</tr>
<tr>
<td>Strictly Confidential (SC)</td>
<td>Visible to a small number of authenticated members only</td>
</tr>
</tbody>
</table>

Such a scheme is clearly high-level, and, as described in the Introduction to Identity Management section, more detailed policy is required for confidential data to set out who exactly is able to view (and create, modify or delete) data. Careful consideration should be given to what is classed as open since many different types of individual may be given credentials even though they would not normally be considered a member of the organisation e.g. a contractor working on a building project.

A primary function of an IdM system is to ensure that such a classification is adhered to internally and externally by systems which receive controlled data. An important part of projects which lead to the collection of new data and/or the integration of new systems is to ensure that data classification analysis is carried out, communicated, and that a risk assessment is carried out along with implementation of any measures which will mitigate any risks.

2.4.2 Organisational units

Many organisational units will require some level of administrative access to the IdM system including devolution of privileges to staff as appropriate. Authority should be granted to a head of unit who then is accountable for how privileges are delegated further. There should be clear rules and processes so that it is evident why privileges have been granted, or, perhaps, refused. There should be high quality training, guidance and support available so that administrators are aware of their responsibilities and know what to do if a problem arises or are otherwise unsure how to apply IdM policies.

2.4.3 End users

Many IdM systems will allow a degree of self-service e.g. updating addresses or changing passwords, however, for non-administrative users the IdM system will remain in the background – if it is operating effectively. That is, access to the systems and services end users need will be granted and revoked in a timely manner, and personal data will only be available to appropriate administrators and only viewed when necessary to carry out required duties.

End users should be given guidance on the importance of protecting their identity and credentials and what
to do if they believe their identity may have been stolen. The consequences of misusing someone else’s identity, or computing and network facilities in general, should also be clear.

2.4.4 Other systems

The IdM system itself will provide identity information to many other systems often operated by staff in other organisational units. As each system is integrated there should be a formal review of what data is transferred between systems and why. Each integration should be documented and any changes subject to review. Documentation should include:

- data classification
- who is responsible for the data
- what the data may be used for
- the process to be followed before a change of use
- guidelines on how to protect the data

2.4.5 Contractors, partners, other third parties

Identity data is at particular risk when it is outside the direct control of the organisation. Data must only be released in a secure manner and to receiving parties who are able to demonstrate adequate information security practice, and, are contractually obliged to maintain the security and confidentiality of data. This is likely to mean that receiving parties have appropriate certification which is regularly renewed subject to satisfactory compliance audits.

2.5 Identity lifecycle and policy areas

The diagram overleaf shows the identity lifecycle and is used to help group policy areas.

(a) Application / invitation

HE and FE organisations process many applications, from staff and students, each year, leading to the collection of identity-related information in both electronic and paper form. In addition, HE and FE organisations may invite individuals to participate in a variety of collaborative activities, such as research, which require those individuals to access facilities and services.

Applications may be tracked in one or more systems and these systems may form part of the IdM system, allowing, for example, applicants to track the progress of their application.

Policy areas / questions and procedures

1. How is fairness in recruitment achieved, monitored and reported?
2. What are the procedures for identity verification?
3. How is entitlement to work / study determined and verified?
4. What proof of identity and entitlement must be recorded?
5. How is access to electronic and paper records controlled?

(b) Unsuccessful application

Many applications will, ultimately, be unsuccessful.

Policy areas / questions and procedures

1. For how long should records be retained for unsuccessful applicants?
Following a successful application, or acceptance of an invitation, an individual normally enters into some contractual arrangement with the organisation. The organisation will then, in general, create a new identity\(^6\) (or, if a returner, re-activate an existing identity), and provide some form of credentials e.g. identity card and / or username / password, which the individual uses to access facilities and services. Individuals may be

\(^6\) Linked to a unique (preferably opaque) identifier that has not previously been used. Re-use of personal identifiers may, inadvertently, allow the new identity to access some of the facilities and services to which the old identity was entitled.
assigned a membership type\(^7\) and their roles and affiliations recorded.

It may be necessary to provide alternative credentials for accessing some facilities and services e.g. when a service is not fully integrated with the central authentication service. When alternative secondary identifiers are required they should be linked to the primary identity in the IdM system.

**Policy areas / questions and procedures**

1. What are the procedures for prior id discovery? i.e. linking a successful applicant with a previous identity e.g. when a new member of staff is also an alumnus.
2. What are all the types of credentials, including physical, allowed?
3. Do different credentials have different Levels of Assurance (LoAs)?
4. How are credentials distributed?
5. What are the policies and mechanisms for generating, changing, disclosing, replacing and revoking credentials?
6. What records of changes are made?
7. What is the policy on the re-use of identifiers e.g. unique id, email address?
8. What is the policy on alternative credentials / identifiers?
9. What general policies e.g. terms and conditions, acceptable use, must be accepted by an individual before they access facilities or services?
10. What advice is given to individuals about where to store business information vs personal information?
11. What are all the categories of users who are entitled to access facilities and services?
12. For each user category how are records created?
13. What happens when a user changes category i.e. applicant becomes student?
14. For each user category who is responsible for determining which facilities and services all members of that category have access to, or must not have access to, and what are those facilities and services?
15. Which facilities and services have additional requirements e.g. additional specific statements to be accepted, or pre-requisite roles and / or training?
16. What data classification scheme is in place?
17. Who is responsible for general (baseline) IdM policy applying to all facilities and services unless superseded by specific policy?
18. For each facility and service who is responsible for specific policy i.e:
   - Type of authentication required and whether any specific functions require additional methods of authentication?
   - Which roles have what permissions for the different functions of a service?
   - How are business process roles implemented technically?
   - Who is responsible for the approval of access permissions?
   - Who is responsible for the administration of access permission (should they be different to the person approving)?
   - How are permissions requested and revoked?
   - What are the expected and maximum acceptable times for access requests to be considered and granted, or revoked?
   - Where are the identities and permissions recorded?
   - What training, if any, is required before using the service?
   - What data is held and how is it classified?
   - How is data synchronised with other services?
   - How is data changed?
   - Who can change what data?
   - How is data linked to data in other systems?
   - What methods are used to ensure accuracy of data recorded about users?

---

\(^7\) Should cover grey areas such as applicants, new recruits who have not officially started, recent leavers, alumni, people on maternity leave or sabbaticals and students who have finished one course but expect to start a new course e.g. undergraduate -> postgraduate, and atypical users.
(d) Role / status changes

Many individuals are members of the organisation over a number of years during which time they may be promoted, change role, move to a different department have temporary leave of absences etc. Each change may be reflected in changes to relationships and affiliations with subsequent changes in entitlement to access facilities and services.

The organisation should take active measures to ensure that members are aware of their general responsibilities with respect to IdM. Particular roles may require specific training.

Policy areas / questions and procedures

1. Who is responsible for registering role / status changes?
2. What are the expected and maximum acceptable times for registering role / status changes?
3. Who is responsible for removing (or requesting removal of) access dependent on an old role / status?
4. Who is responsible for granting (or requesting) access appropriate to a new role / status?
5. What policies and procedures exist to ensure that members of the organisation are aware of their general and specific responsibilities, with respect to IdM, and, in particular, changes in legislation and / or advice?

(e) Integration

An IdM system is designed to be an authoritative central hub of identity information. External services may access information through APIs or directory services, or data may be provisioned to the external service. It is crucial to ensure that information security is maintained when data is in transport and when stored in a new location. Changes in the IdM system should be propagated to external systems in a timely manner. The ease and speed of propagating changes may be a factor when procuring systems which need to be integrated with the IdM system.

Policy areas / questions and procedures

1. What is the procedure by which IdM system requirements are taken into account during procurement of other systems?
2. What is the procedure for requesting integration between a new service and the IdM system?
3. Who is responsible for signing off a request for integration?
4. Who is responsible for ensuring that data classifications are respected?
5. What are the technical requirements for integration e.g. encryption?
6. Who is responsible for implementation of the integration?
7. Who is responsible for certifying the integration?
8. What are the procedures for monitoring provisioning and verifying that external systems are using current data?

(f) Leaving the organisation

In many cases it is predictable when an individual will leave the organisation, or there is reasonable notice e.g. retirement, end of contract, end of studies, resignation and redundancy. Individuals should be reminded, in good time, to retain any personal information held in the organisation's data stores and ensure that business information is moved to appropriate data stores where colleagues have access.

Once an individual leaves the organisation they should be removed from external systems, possibly after a period of first being disabled\(^8\). An individual may return to the organisation and be assigned their old identifier, but they should not necessarily have access to the same facilities and services as before.

\(^8\) Some systems may need to retain identity information even if the identity should no longer be able to access the system e.g. library system maintains records to enable collection of outstanding fines. Some services may offer a grace period so, for example, students may read email for a period after the end of their course.
In cases of suspension, dismissal, failure to complete studies or due to disciplinary sanctions there may be a need to remove some, or all, access to facilities and services quickly.

**Policy areas / questions and procedures**

1. How long after official leaving dates do credentials become invalid?
2. Which facilities and services are individuals (of different member types) allowed to access between their official end date and their credentials becoming invalid?
3. What are the policies and procedures, and who is responsible, for ensuring that information of relevance to the organisation (e.g. business correspondence, intellectual property, research data etc) is moved from personal data stores to appropriate alternative locations prior to an individual’s leaving date?
4. How long are personal data stores maintained on live systems and archive before destruction?
5. What is the policy for accessing personal data stores after an individual has left the organisation – including handling requests by the owner?
6. How long are records, including paper files, retained for?
7. What are the policies regarding release of identity information to third parties e.g. for references?
8. Where there is a need for continuing correspondence between the organisation and leavers, what procedures are in place for ensuring up-to-date contact details?
9. What is the procedure for alumni or others to be removed from mailing lists?
10. What are the policies and procedures for removing access to facilities and services for disciplinary reasons?
3 Identity Management Systems, Components and Functions

3.1 Introduction

Executive Summary

This section explains the technical components and functions, in general terms, of Identity Management required by an academic institution. It would form suitable background reading for IT service managers and staff who will be responsible for commissioning, implementing or maintaining IdM systems and data.

Section contents

- **3.1 Introduction**: Describes the requirements for an IdM system.
- **3.2 Core IdM system components**: Describes the logical functions of an IdM system.
- **3.3 Federated access**: Gives an overview of federated access, concentrating on its implementation in Shibboleth.
- **3.4 Provisioning in more detail**: Describes how an IdM system needs to be integrated with external systems.

This section focuses on the technical aspects of an IdM system. The functional aims of such a system are to deal, securely, with the areas of IdM outlined in the IdM definition:

- managing identity information
- integration
- security and access control
- compliance and governance

From a technical perspective these areas can be expanded:

- manage identity attributes and the identity life cycle
- integrate identities with disparate systems
- control access to systems and facilities, including:
  - access to identity attributes
  - access by external identities
  - provision of identity attributes to external services
- provide the means to determine:
  - when identity information changed
  - what the changes made were
  - who made the changes
- provide the means to detect misuse of the system e.g.
  - malicious attacks
  - breach of policy
- provide the means to monitor the health / status of the system

in accordance with a policy and procedure framework.

This section of the Toolkit describes a system for achieving these aims. The system is designed on the premise that by modelling identities and their roles in an authoritative central system, many manual and system specific processes can be re-cast as variants of a small number of processes which share common components. Further, given that policy, systems and organisations change over time a key feature of an IdM system is flexibility.

3.2 Core IdM system components

The components described here correspond to distinct logical functions of an IdM system, rather than the way software components are designed and bundled together.
### 3.2.1 Identity repository and lifecycle management

Common features include:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User categories</td>
<td>Most organisations will classify users in one or more categories. The categories are likely to determine what data is stored about an individual, feature in workflow rules and feature in access control policies</td>
</tr>
<tr>
<td>User records</td>
<td>The actual data held about individuals</td>
</tr>
<tr>
<td>Credential management</td>
<td>Creation and storage of passwords, certificates etc. including enforcement of policies such as password strength</td>
</tr>
<tr>
<td>Self-service</td>
<td>Ability for users to self-register and/or maintain some identity attributes, possibly subject to workflow</td>
</tr>
<tr>
<td>Workflow</td>
<td>Rules which govern the lifecycle of identities e.g. a self-registered identity may require further verification</td>
</tr>
<tr>
<td>Organisation modelling</td>
<td>Most organisations have some structure and degree of hierarchy. An IdM system will generally allow modelling of an organisation's structure</td>
</tr>
<tr>
<td>Provisioning/synchronisation</td>
<td>In practice many computer systems hold some identity attributes. It is important that changes are reflected through all systems in a timely manner, including the removal or disabling of accounts as appropriate</td>
</tr>
<tr>
<td>Auditing and reporting</td>
<td>The logging of changes to data, workflow steps, and the ability to review past actions</td>
</tr>
</tbody>
</table>

### 3.2.2 Authentication service

Common features include:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential validation</td>
<td>Ability to verify passwords, digital certificates, biometric data etc</td>
</tr>
<tr>
<td>Level of Assurance (LoA)</td>
<td>How certain can a system be that an authenticated electronic identity is being operated by the genuine real world identity? Some methods of authentication and/or the practice of identity management at organisations may be more prone to misuse than others. An authentication system may rate the LoA, which, in turn, allows authorisation services to implement appropriate policies given the importance / sensitivity of the resource being accessed.</td>
</tr>
<tr>
<td>Single sign on (SSO)</td>
<td>Ability to use the same user id and credentials for all systems. May be configured to allow automatic authentication such that, after an initial login, further resources may be accessed without the user being prompted for credentials</td>
</tr>
<tr>
<td>Proxy authentication</td>
<td>Ability for a system where an identity has authenticated, to present credentials, on behalf of the identity, to a second resource i.e. a user logs into a Portal which is then able to authenticate as that user to many different data sources</td>
</tr>
<tr>
<td>Federated access</td>
<td>The ability to generate credentials which may be used to authenticate a user at an external service, or to consume credentials and authenticate identities</td>
</tr>
</tbody>
</table>

9 Authentication may, or may not allow a resource to directly map an electronic identity to a real world identity. It may be sufficient to trust that an electronic identity belongs to a partner organisation.
### 3.2.3 Authorisation service

Common features include:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules</td>
<td>Machine readable logic which the service executes to determine whether an identity may access a resource or particular feature/function of a resource.</td>
</tr>
<tr>
<td>Policy</td>
<td>Set of rules which apply to a resource</td>
</tr>
<tr>
<td>Roles</td>
<td>For large complex organisations managing rules for individual identities becomes impractical. By mapping identities to roles, general policies applying to many identities may be implemented with a few rules</td>
</tr>
<tr>
<td>Groups</td>
<td>Similarly to roles there are benefits in applying policies to groups of identities rather than individuals</td>
</tr>
<tr>
<td>Delegation</td>
<td>In the same way that authority is devolved through an organisation an IdM system should be able to apply policies which devolve appropriate administrative authority in a way suitable to the structure of the organisation</td>
</tr>
<tr>
<td>Proxy</td>
<td>In some cases a person may need to act on behalf of a superior, or for a colleague who is ill, suspended, on sabbatical etc. It may be possible to temporarily transfer authority to another identity</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Most systems are designed with their own authorisation system. Some will have hooks to enable authorisation decisions to be resolved by an external service, however, in the case where a system lacks such a function it may be necessary to translate and provision access control rules to external systems in a format that can be consumed by that system.</td>
</tr>
<tr>
<td>Auditing and reporting</td>
<td>The logging of authorisation requests and results, and the ability to review when services were accessed, or which identities had access to a service at a given point in time. This may be used to detect attacks on the system.</td>
</tr>
</tbody>
</table>

### 3.2.4 Directory service

Common features include:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity discovery</td>
<td>Ability to browse or search for identities. Restrictions are likely to be imposed for anonymous clients</td>
</tr>
<tr>
<td>Lightweight Directory Access Protocol (LDAP)</td>
<td>Many IdM systems make data available through LDAP</td>
</tr>
<tr>
<td>Schemas</td>
<td>LDAP allows the definition of arbitrary object types. In practice, a core set of object types which allow organisations and people to be represented have been developed and are likely to be available in any LDAP implementation. A group of related object types are referred to as a schema. In HE some additional schemas have been developed: eduPerson, eduOrg, eduCourse. Sector-specific schemas can be difficult to define (reach agreement on) or may require extension to be useful in specific contexts. However, they are</td>
</tr>
</tbody>
</table>

28 of 123
valuable because they are designed to solve common problems once, provide a common vocabulary and make it easier to integrate with other software which can be designed to support standard object types.

Virtual directory
Allows disparate data sources to appear as one directory e.g. some queries may be mapped directly to a relational database query.

### 3.2.5 Groups service

Common features include:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic groups</td>
<td>Lists of identities are generated, on request, by performing a query</td>
</tr>
<tr>
<td>System maintained groups</td>
<td>Lists of identities are maintained and fully enumerated within the system by a loader which makes decisions based on attributes such as department and course</td>
</tr>
<tr>
<td>Ad hoc groups</td>
<td>User maintained groups. Typically groups which cannot be automatically derived from identity attributes</td>
</tr>
<tr>
<td>Personal groups</td>
<td>Groups which do not have formal organisational significance but allow users to share information informally. In effect much of the social web is based around personal groups i.e. lists of friends. Personal groups are also ad hoc, however, not all ad hoc groups should be considered personal groups</td>
</tr>
<tr>
<td>Inheritance</td>
<td>If group B is a member of group A then group A inherits all the members of B</td>
</tr>
<tr>
<td>Name space</td>
<td>Groups may exist in a hierarchical name space in order to facilitate delegation of privileges, facilitate browsing and searching, and to prevent name collisions between organisational units</td>
</tr>
<tr>
<td>Self-service</td>
<td>Users may be able to opt in or out of groups e.g. optional mailing lists, thus facilitating customisation</td>
</tr>
<tr>
<td>Membership expiry</td>
<td>Ability to set an end date on a membership</td>
</tr>
<tr>
<td>Attributes</td>
<td>Groups may have attributes to facilitate searching and to allow selective integration with other systems</td>
</tr>
<tr>
<td>Authorisation</td>
<td>The membership lists of some groups may be sensitive - indeed the existence of some groups may be sensitive, so a groups service would be expected to provide control over who can view and/or update groups and their memberships</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Groups can be considered identities in their own right and the goal would be to ensure that groups are created once and maintained in a central repository but are available, up-to-date, in all relevant systems</td>
</tr>
<tr>
<td>Auditing and reporting</td>
<td>Groups are often used to control access to services so it is important to be able to determine how, when and by whom group memberships were created/removed</td>
</tr>
</tbody>
</table>

### 3.2.6 Asset repository

Common features include:
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arbitrary objects</td>
<td>Many IdM repositories allow arbitrary objects to be defined. They are of value because they allow authorisation rules to, for instance, control physical access to buildings or rooms using an id card. They can also control who can book rooms or other physical resources.</td>
</tr>
<tr>
<td>Object types</td>
<td>Each object will have a type which defines a set of attributes that are appropriate for describing the object</td>
</tr>
<tr>
<td>Standard types</td>
<td>An asset repository will have a library of standard object types e.g. building, room, printer</td>
</tr>
<tr>
<td>Custom types</td>
<td>Organisations may need to define new object types or extend standard types</td>
</tr>
<tr>
<td>Asset relationships</td>
<td>Assets may be grouped e.g. by location or ownership. Such groupings make it easier to browse / search for assets and allow for fine-grained authorisation rules. In particular assets should be mapped to the organisational model</td>
</tr>
</tbody>
</table>

### 3.2.7 Overview diagram

In principle, the components introduced above may be loosely coupled and/or may be provided by different vendors/open-source projects. The diagram below depicts this, showing a logical separation of functions.

![Overview diagram](image-url)
3.2.8 Consolidated overview with access control

In practice, many vendors will provide an integrated solution which may be managed using a single user interface and which stores all data in a single physical repository. The diagram below depicts this approach and, in addition, shows how an IdM system interacts with external systems.

(a) Load identities
Ideally all identities would be created and managed within the IdM system, however, in practice this may not always be possible or desirable given the impact on well-established legacy systems and processes. Further, most systems are designed to work standalone i.e. they provide sufficient IdM tools in a self-contained installation to allow users to be registered with local credentials, although they may, through APIs / plugins, allow some integration with existing IdM systems. This creates the potential for individuals to have disconnected identities across a range of systems i.e. even if systems are initially provisioned from a central IdM system, the ability to manage identity attributes in provisioned systems will, over time, lead to discrepancies and a lack of confidence in the accuracy of the IdM system. This in turn leads to fragmentation i.e. identity bunkers where system owners do not trust any data other than that maintained in their own system. In addition, atypical users may even be registered independently on separate systems. Due to the ease of changing, and even creating, identities within systems there is likely to be resistance to processes which require that identities are created or changed in a separate IdM system, particularly if the new or changed identity is not provisioned in a timely manner.

(b) Attempt access
An end user attempts to run protected software, access a protected web site, or enter a building/room.

(c) Who are you?
Credentials may be typed or provided automatically by the user agent e.g. browser provides certificate or swipe card system reads bar code on Id card. The authentication service decides whether to accept the credentials. In the case of federated access there may be a where are you from? (WAYF) step in which the user selects their organisation in order to authenticate. The protocols agreed to by federation members allow the access point to trust external authentication and user attributes provided by the identity provider.
The diagram shows the authentication service accessing the identity repository. In practice this may occur indirectly via the directory service where standard vendor-independent protocols are available.

(d) Check allowed
The resource applies access control rules to determine if the user has access to, or what restrictions should be in place to limit use of, a resource. Such rules may depend on attribute values made available upon authentication.

The diagram shows the authorisation service accessing the identity repository. In practice this may occur indirectly via the directory service where standard vendor-independent protocols are available.

(e) Grant access
If allowed the end user accesses the resource with appropriate fine-grained controls.

(f) Lookup identities
Some applications e.g. mail clients / calendars, allow end users to search for other users. Further, many vendors support access control policies based on directory service query results

Once an IdM system has been implemented it should influence future system procurements i.e. how easily and satisfactorily can a new system be integrated?

3.3 Federated access
The diagram overleaf and the following sections provide an overview of how identities from one organisation may use Shibboleth to gain federated access to services hosted by another organisation. Membership of a federation places obligations on members which allow members to trust identity assertions provided by other members.

An organisation may also choose to use this model internally. The advantage of this approach is that it provides a single, consistent means of authenticating users and implementing access control.

The Shibboleth-based UK Access Management Federation for Education and Research is supported by JISC, with some support for the schools sector from JANET(UK). The federation website gives a list of benefits for joining the federation10.

3.3.1 Shibboleth
Shibboleth11 is an open source product developed for HE/FE by Internet2 and is based on the Security Assertion Markup Language (SAML). Other implementations of SAML are available12.

(a) User attempts to access a resource protected by Shibboleth
In Shibboleth terms an organisation which hosts services operates components which, collectively, are known as a service provider. When an unauthenticated user attempts to access a resource, the service provider initiates the steps below. All steps must succeed before access to the resource is granted.

An organisation may present a number of different services through a single web address. A service may be integrated directly into a web server or the web server may act as a proxy to a service. Typically a service provider will include a component which is installed as a web server plug-in. This approach avoids having to incorporate the component in individual services, though that approach may also be used.

(b) Service provider invokes WAYF service
A service provider maintains a list of federation members and their associated web addresses and public keys. The list of federation members is presented to the user, typically as a web form.

10 http://www.ukfederation.org.uk/content/Documents/Benefits
11 http://shibboleth.net/
12 A number of open source implementations are listed at http://saml.xml.org/wiki/saml-open-source- implementations. In addition some companies have developed SAML gateways to their service offerings e.g. Google (https://developers.google.com/google-apps/sso/saml_reference_implementation_web) and Microsoft (see, for example, http://msdn.microsoft.com/en-us/library/ms730908).
(c) User selects their home organisation
When selecting their organisation a user may have the option to have the WAYF service remember (by means of a cookie) the user’s organisation for a period of time. This option makes subsequent access via the service provider easier.

(d) User redirected to identity provider
In Shibboleth terms an organisation which validates user identities, operates components which are, collectively, known as an identity provider. Once a user has selected their home organisation, the WAYF service redirects the user to the web address of the identity provider for that organisation.

(e) Identity provider requests authentication
The identity provider itself is a protected resource and will initiate an authentication request.

(f) User provides credentials
Typically the user presents credentials to a single sign-on service.

(g) The home organisation verifies the user’s credentials
Successful authentication provides access to the identity provider

(h) Identity provider processes request
The identity provider generates an opaque, transient identifier (handle) associated with the authenticated
(i) **User presents handle to service provider**

The service provider attempts to validate the handle and obtain attributes for the user.

(j) **Handle passed to attribute requester**

Internally a separate component (attribute requester) deals with the handle.

(k) **Attribute requester tries to obtain user attributes**

Until now the user's web browser has been responsible for the transfer of data. Now, the attribute requester connects directly to the identity provider sending the handle and, possibly, a request for specific attributes. The identity provider verifies that the handle is valid and applies appropriate attribute release policies before returning any attributes.

(l) **After accepting the handle and receiving attributes the user accesses the resource**

The return of attributes confirms that the identity provider has verified the identity of the user (though the attributes returned may not allow the user to be identified)

(m) **The resource enforces appropriate access policies**

The resource may refer to the service provider's authorisation service before granting access and to determine the level of access.

### 3.3.2 Other considerations

Federations have tended to be developed at a national level for specific sectors. However, HE organisations often have international links which raises the issue of supporting multiple federations, and trust between federations. Also, what happens when individuals belong to organisations which are not members of a federation - possibly because the infrastructure does not exist nationally?

Federated identities are, in effect, owned by their identity provider. However, many individuals have affiliations to two or more organisations - some of which may be virtual in nature e.g. a research group. Currently there is no mechanism for linking identities for an individual which come from distinct identity providers and providing a composite set of attributes. This means that depending on the identity provider an individual uses to gain access to a service, the individual may have different levels of access. Certainly the service provider cannot provide a consistent personalised experience and any user customisations would have to be repeated for each federated identity.

Given that identities are closely tied to organisations, there may be consequences for virtual organisations when an individual changes place of employment or study but maintains a role in the virtual organisation i.e. the need to be able to map a different federated identity to an identity referenced within the virtual organisation.

### 3.4 Provisioning in more detail

There are several approaches to integrating with external systems. In practice, a combination of methods will be implemented due to system limitations, timeliness of changes, user training issues, resource availability for process re-engineering, or, to do otherwise, would add unnecessary complexity or be cumbersome.

The diagram overleaf illustrates potential data flows. Each flow is labelled (a) to (k) and explained in the following sections.

(a) **Direct API access**

Systems of record may directly, or indirectly (through an intermediate script) load data directly to the IdM system using APIs provided.

External systems could, in principle, obtain data / resolve authentication or authorisation queries directly through the IdM system APIs. Such tight coupling of systems may compromise the availability of systems during maintenance periods.
(b) Internal IdM system components use direct API access
Authentication / authorisation services may provide their own user interface to manage credentials / authorisation rules. Direct API access may be required to store changes in the IdM repository.
Similarly to (a), authentication / authorisation queries may be resolved through direct API access, however, this has the same drawback as (a) i.e. compromise of system availability during maintenance periods.

(c) IdM system actively provisions/synchronises data with external systems
Here an agent (provisioning engine) listens for changes within the IdM system, or periodically queries for changes.

(d) Internal IdM system components store local data
Individual internal systems may have their own database. This allows such services to operate even if the
IdM repository is unavailable.

**(e) Changes in IdM system provisioned to directory service**

The directory service can operate even when the IdM repository is unavailable.

**(f) Internal IdM system components may rely on the directory service**

Rather than maintain their own data store, internal components may read data from the directory service. This decouples the services from the IdM repository and saves some duplication of data.

**(g) IdM system supports multiple targets**

One would expect the provisioning engine to have a modular architecture whereby custom modules may be written to cope with new targets. Provisioning may be sequential i.e. each target is provisioned in turn, or concurrent i.e. targets are provisioned in separate threads or processes. A commercial IdM system would be expected to provide provisioning modules for common targets. This may require the installation of agents on target systems.

- Many Windows-based systems are designed to work with Active directory
- Many systems are RDBMS-centric and have few or no LDAP capabilities. It may be necessary to map IdM data to various schemas depending on the capabilities of external systems that require RDBMS access to data
- It will often be desirable to manage local system accounts through the IdM system
- External systems may have APIs which can be exercised directly by a provisioning module
- External systems may have batch update features or it may be possible to write scripts to load files

**(h) External systems should use central authentication/authorisation services**

Many systems support multiple authentication services; however, fewer systems integrate with external authorisation services. Where an external authorisation service cannot be used, it may be possible to model all or part of the system’s access model in the IdM system and provision to the external system. The advantage of this approach is that there is a central view of access privileges. It may also be possible to map high level policies/rules to system specific policies/rules in a number of systems easing the administrative work load, i.e. if user X is allowed access to financial information for department Y which may be accessed in systems A, B and C, a single high level policy can be applied to user X without having to apply individual policies for A, B and C.

**(i) External systems should use central directory services**

Directory services are designed for fast read access and high availability. They reduce the need for individual systems to hold local copies of data. Many systems are available which can take advantage of directory services.

**(j) Message queues can provide an alternative to direct provisioning**

As changes happen in the IdM repository notification messages are sent (published) without waiting for a response. External systems may listen for (subscribe to) messages and act accordingly upon receipt. Message queues can be designed to guarantee delivery of messages i.e. they can resend messages if a system was unavailable, or unreachable.

This approach provides some resilience for service / network outages, and provides loose coupling which makes it easier to integrate new (capable) systems.

**(k) The IdM system can also listen for messages**

External systems may send messages which can be consumed by other systems including the IdM system.

### 3.4.1 Synchronisation

There are two ways external systems may become out of synch with the IdM system:

1. Due to system downtimes, network errors, or bad exception handling some IdM repository changes may not be provisioned to one or more targets
2. Data is modified directly in the external system
Periodic batch updates may resolve the former, however, provisioning modules may be designed to compute differences and make only necessary changes.

When data can be modified directly in an external system – probably the default situation – there is always the problem that changes may be overwritten. Provisioning modules may be configured to generate alerts so an administrator can make a decision, or it may be possible to configure rules which allow the module to reconcile the differences.
4 Defining Institutional Requirements:

4.1 Introduction

Executive Summary
This section outlines the general technical requirements an institution should specify for the implementation of IdM. These cover the key areas for any IT system such as usability, availability, integration, security and sustainability. For each key component of an IdM system (credential management, single sign on, provisioning/synchronisation, workflow and authentication/authorisation) specific requirements are listed. It is recommended that the specific requirements be collated as part of the audit process, as they will vary from one institution to another depending on existing IdM practices and systems. The language used in this chapter implies a packaged solution, however, an IdM system may be composed of components from different suppliers and include systems developed in house. Whatever the solution significant local customisation and integration will be required.

Section contents:

• **4.1 Introduction**: Describes how this section helps clarify institutional requirements for an identity management system.

• **4.2 General requirements**: Describes requirements which apply to an IdM system as a whole.

• **4.3 Functional requirements for IdM components**: Describes functional requirements for the IdM system components described in the previous section.

• **4.4 Generating specific institutional requirements**: Suggestions for taking this generic system as the basis for specific institutional IdM requirements.

The Introduction to Identity Management section introduces some of the key IdM components and concepts, and the Identity Management systems, components and functions section presents an ideal model, i.e. the model to aim for if starting with a clean slate and assuming that there are in existence appropriate systems which can be easily integrated.

Few, if any, organisations are in a position to start from scratch or would find that their preferred systems solutions always integrate easily. An IdM system is likely to be introduced in stages and will accommodate some legacy systems and processes. For this reason it is not possible to produce a definitive set of requirements which are appropriate for all organisations. The use of terms such as must, should and may indicates the importance attached to individual requirements by the authors, however, ultimately, each organisation will have to determine the importance of each requirement in their own context.

Here a set of functional requirements is presented for each IdM component. The requirements emphasise what would be expected in an ideal system, but also highlight key choices which can be made to enable progress in a less than ideal world. These may be useful in defining the objectives of an in-house implementation project; or in detailed specifications to suppliers.

The language used in this chapter implies a packaged solution, however, an IdM system may be composed of components from different suppliers and include systems developed in house. Whatever the solution significant local customisation and integration will be required.

Statements of requirements are listed in plain text.

*Explanations and reasons for each are presented in italics.*

4.2 General requirements

4.2.1 Usability

An IdM system must provide a comprehensive user interface that allows all objects and services to be configured and managed.
Allows a range of users with differing technical skills to use the system without having direct access to configuration artefacts.

The user interface may be web-based.

Easier to deploy to a large user base and accessible from anywhere.

The user interface should be customisable.

Allows organisation specific branding and terminology, and creation of custom screens to reflect local policies and workflows.

It should be straightforward to view and revoke all of a user’s access privileges.

Reduces the risk of malicious activity by individuals subject to disciplinary procedures.

It should be straightforward to view activity related to an identity.

Supports troubleshooting. Also, if users are aware that their activities can be reviewed this acts as a deterrent to misuse.

4.2.2 Availability

Given the central importance of an IdM system it must be resilient and highly available.

Even short outages will disrupt essential activities and potentially breed mistrust and resentment. The system architecture and implementation should aim to maintain as many services as possible when essential upgrades and patching (software, operating systems and databases) are required.

Rapid disaster recovery is essential.

Prevents key processes grinding to a halt.

Clustering services may allow individual service instances to be taken offline and upgraded or patched.

Provides flexibility when managing systems which need to be available 24/7.

Separation of managed data from runtime data should be considered

May allow authentication, authorisation and directory services to continue in the absence of management functions. That is, if managed data is provisioned to a read-only directory, and external systems / authentication and authorisation services are designed to obtain runtime data from the directory, they can function even when the identity repository and lifecycle management functions are not available.

4.2.3 Integration

When provisioning data to a directory it should be possible to specify one or more representations, or a virtual directory may map queries from expected to actual representations.

Systems which can take advantage of LDAP may make assumptions about how data is stored in a directory. The system should be flexible to maximise the potential for straightforward integration.

For systems which do not support LDAP significant effort may be required to achieve integration. An IdM system must provide a means of determining what has changed and needs to be synchronised. It should provide scheduled asynchronous and near real-time hooks which allow integrators to plug in custom provisioning code. Such code may be able to exercise APIs in target systems, however, in other cases it may be necessary to produce output files which are then loaded, by another process, into a target system. The IdM system should be able to produce a well documented machine readable representation of object changes e.g. defined XML format such as SPML.

The system should be flexible to maximise the potential for straightforward integration.

The IdM system must provide a comprehensive set of APIs. APIs should conform to industry / sector standards where appropriate. APIs should be available in a programming language neutral way, e.g. as web services. APIs may also be provided in the programming language in which the IdM system was developed. APIs may allow systems of record to update identities, assets, organisational structures and policy rules.

The system should be flexible to maximise the potential for straightforward integration.
4.2.4 Security
The IdM system should use its own authentication and authorisation services to ensure appropriate security. *Avoids duplication, but, more pertinently, the outward facing authorisation service should be able to cope with the security model of the IdM system otherwise it may well not be sufficient to work with security models in other systems.*

In addition to general auditing and reporting the ability to monitor IdM system usage and generate alerts for suspicious patterns of use should be considered. *Better to catch issues early rather than after the system has been compromised.*

4.2.5 Supportability
It should be possible to version control configuration artefacts. *Facilitates trouble shooting if system behaviour changes in unexpected ways.*

It should be possible to export and import configuration artefacts. *Facilitates upgrades and allows changes in test systems to be migrated to production systems.*

It must be possible to find and diagnose faults quickly through generation of alerts and appropriate logging. *Leads to reduced and shorter outages.*

The IdM system must be well-documented - both user and system documentation. *Reduces implementation time. Reduces user errors and allows full range of features to be exploited.*

There must be sufficient internal and/or external support staff to maintain the system. *Avoids over dependence on one or two individuals.*

The IdM system should use appropriate standard protocols and tools where available. *Easier to find staff with appropriate skills and/or find appropriate training courses.*

4.3 Functional requirements for IdM components

4.3.1 Identity repository and lifecycle management

**Identity creation**

1. Must allow the creation of new identities
   *Otherwise local system-specific accounts will be set up which will, most likely, be badly managed*
2. Must provide tools to prevent duplicate identities
   *Duplicate identities can lead to incorrect management of identities due to incomplete information*
3. Must provide a means to reconcile duplicate identities
   *No process to avoid duplicate identities is likely to be 100% successful so it is important to have the ability to merge records to obtain a single complete identity which can be effectively managed*

**Credential management**

1. Must allow secure creation and storage of credentials
   *Organisations have a duty to prevent misuse of systems. If credentials are not protected they may be stolen and used to impersonate their owners.*
2. Must support common credential types, for example passwords, digital certificates, biometric data, cards
Distinct systems, data and facilities have different degrees of value / sensitivity. Support for multiple credential types allow the organisation to use credentials which are appropriate to the level of risk.

3. Should be extensible i.e. quickly manage new credential types and formats

   Future proofs against the advent of new technology and credential types

4. Must have configurable policies e.g.
   i. password strength
   ii. change password on first use
   iii. change password every configured period of time

   Provides flexibility, preventing the technology becoming a barrier to implementation of desirable policies.

5. Must allow non human service accounts

   Otherwise credentials for individuals may be used insecurely e.g. in configuration files. Many organisations run unattended batch processes and it is desirable to distinguish actions resulting from these processes from actions carried out by a real user.

Workflow

1. Should allow configurable rules for identity:
   i. creation
   ii. updating
   iii. activation
   iv. provisioning
   v. suspension
   vi. de-duplicating
   vii. archiving
   viii. deletion
   ix. restoration
   x. self-service i.e. self-registration, attribute maintenance

   Future proofs against changes in policy, including those required by legislation, and provides flexibility for applying different policies to different types of users

2. May allow integration with third-party workflow management applications

   Allows the organisation to use their preferred system, or to adopt a best-of-breed workflow system in the future. Allows more efficient integration between disparate systems

Organisation modelling

1. Must allow the organisational hierarchy to be defined

   Many implicit rights derive from an organisation’s structure, however, different rules / policies may apply in different parts of the organisation. Correctly modelling the organisation ensures that rules / policies are applied correctly

2. Must allow devolved management of the organisational hierarchy and identities where appropriate

   Reduces the need for a large central organisation which could become a bottleneck. Reduces errors because administrators deal with the parts of the organisation they are responsible for. Increases organisational efficiency by reducing the lag involved in generating and processing requests

3. Should allow re-organisation of hierarchy

   All organisations change over time and the IdM system should facilitate such changes rather than
act as a barrier to that change

4. Should allow for identities to belong to multiple organisational units

   Individuals may have more than one role in an organisation and failure to model such complexity increases the risk of errors when managing access to systems and facilities

5. Should allow fine-grained groups management including
   i. dynamic groups – rule / query based memberships determined at run time

      Can be more efficient to manage large groups which are easily defined by well-understood attributes e.g. staff / student
   ii. static groups – user or system maintained groups

      Allows ad hoc groups to be maintained. Allows more complex rules to be applied when determining group memberships
   iii. control of group and membership visibility

      Some work within the organisation may be sensitive e.g. animal experiments. Exposing group memberships may pose a risk to members
   iv. provision of self-service groups i.e. members can opt in and opt out

      Allows users to control whether they receive specific kinds of information according to their interests

**Provisioning/synchronisation**

1. Must support batch and real-time provisioning to a standard LDAP service

   Prevents the LDAP service getting out of synch with the IdM system whilst ensuring up-to-date identity information, including access rights

2. Should support batch and real-time provisioning to a range of common systems i.e. relational database management systems (RDBMS), Active Directory

   Typical organisations have a heterogeneous range of legacy systems. The IdM system should provide tools to help integrate with these systems

3. Should provide real-time notifications of identity changes

   Improves organisational efficiency and improves user experience, by reducing delays

4. May provide a provisioning engine with plugins for standard targets and an API for custom plugin development

   Allows tailored provisioning solutions

**Auditing and reporting**

1. Must log who made what changes and when

   Makes it possible to troubleshoot consequences of changes. Storing details of the last changes is often insufficient to understand how data has changed. If users know that their activity is logged they are less likely to misuse the system.

2. Should provide report on changes made by a specified identity

   Useful for an individual, or their manager to review activity.

3. Should provide report on changes made to an identity

   Useful to see how an identity has changed over time - may help to explain intermittent issues.

4. May allow rollback of changes to a point in time

   Useful to rectify a mistake

5. Should report on an identity as it existed at a point in time
Useful for understanding what the identity was able to access e.g. in case of a dispute

### 4.3.2 Authentication service

#### Credential validation

1. Must not expose credentials in a way which allows their misuse e.g. clear text passwords.  
   *Organisations are legally obliged to protect personal data.*

2. Must recognise irregular patterns of usage e.g. systematic trial and error of username/password combinations, and  
   i. provide alerts  
   ii. account locking  
   *Organisations should be pro-active in monitoring systems for mis-use and take appropriate measures to block attacks*

#### Level of Assurance (LoA)

1. Should provide an accurate LoA when requested.  
   *Likely to become a requirement when working across organisational boundaries*

2. Should support configurable rules for determining access based on LoA. Please refer to the first chapter for more information about LoA.  
   *Allows the organisation to use a level of security appropriate to the level of any risk*

#### Single sign on

1. Should support the use of the same credentials, where practical, across all systems.  
   *Much easier for users. Reduces support calls about forgotten passwords. Makes it easier for users to change their password*

2. Should allow administrator and/or user and/or resource to specify whether credentials must be re-presented to gain access to all or particular resources.  
   *Reduces the risk that someone can inadvertently or maliciously use someone else’s identity*

3. Should use time-limited, single use tokens rather than exposing user credentials to resources.  
   *Prevents snoops intercepting a token and re-using it.*

4. Should provide single sign off i.e. end all current sessions for an identity  
   *Browsers may remain logged into a service even if the user navigates away or logs out of a different service. Single sign off reduces the risk of inadvertent or malicious access to systems*

#### Proxy authentication

1. Should support the ability for a system where an identity has recently authenticated, to present credentials, on behalf of that identity, to a second resource.  
   *Systems do not need to store primary credentials, such as passwords. Services may be secured in one way. More secure than systems which, for example, take a user id as a parameter. Supports application such as portals which aggregate content*

2. Should be able to configure which resources may use/accept proxy authentication  
   *Allows the organisation to configure trust and reduces the possibility of a rogue application being used to secretly retrieve data*
**Federated access**

1. Must support membership of the UK Access Management Federation for Education and Research
   *This is the national federation of which the majority of the sector are members*
2. Should support membership of other federations.
   *Collaboration is often international*
3. May support other federation schemes e.g. Liberty Alliance—Identity Web Services Framework (ID-WSF)
   *There are many initiatives aimed at giving individuals more control over their identity.*
4. Should allow a range of attribute release policies including user-controlled policies
   *Different services require different attributes and it is not practical to manage all of these centrally*
5. Should allow proxy authentication
   *There are benefits to using federated access internally within an organisation, however, lack of proxy authentication would limit its application to some services*

**Auditing and reporting**

1. Must log who authenticated, to which resource, when and from where, and using which credentials, with which LoA
   *Provides means to look for and investigate misuse*
2. Should report on authentications made by an identity
   *Can be used to detect misuse or troubleshoot access problems*
3. Should report on authentications to a resource
   *Can be used to detect misuse or troubleshoot access problems. May be helpful for capacity planning*
4. Should provide reports to highlight possible misuse
   *Automated summary reports provide consistency and a quick means to check if there are issues*

**4.3.3 Authorisation service**

1. Must allow scoped rules based on identity attributes (including roles and group memberships).
   *Facilitates automatic access controls. Individuals may have the same role but scoped to a different department*
2. Must support multiple roles per identity
   *Supports real-world complexity where people often have multiple roles*
3. Should support hierarchical roles i.e. roles which inherit from parent roles
   *Makes it easier to manage roles by reducing duplication*
4. Should support rules which can limit assignment of conflicting roles
   *Provides flexibility e.g. the organisation could prevent a requisitioner from authorising their own requisitions*
5. Roles should support attributes
   *Supports scoping and limits*
6. Should dynamically and automatically change access rights based on changes in identity roles
   *Increases organisational efficiency by reducing delays and manual intervention on individual systems*
7. Must allow access rules to be applied to roles and groups
More efficient than applying to individuals

8. Should allow access rules to be applied to individual identities
   Supports exceptions

9. Should support proxy delegation but enable control of who may delegate and to whom.
   Supports organisational flexibility whilst providing control

10. Should be able to model access control in arbitrary systems.
    Supports legacy systems

11. Should support batch and real-time provisioning to standard directory services.
    Many systems support LDAP

12. Should support batch and real-time provisioning to a range of common systems i.e. relational
    database management systems (RDBMS). Active Directory
    Many systems do not provide a means of making external authorisation checks

13. Should provide real-time notifications of changes to roles and authorisation rules
    Allows changes to be propagated

14. May provide a provisioning engine with plugins for standard targets and an API for custom plugin
    development to allow tailored provisioning solutions.
    Facilitates integration with systems

15. Must log all authorisation requests and responses. Should log configured meta data e.g. ip address.
    Useful for troubleshooting and detecting misuse

16. May log applicable rules used to reach a decision.
    Useful for troubleshooting

17. Should be able to report on all policies / rules which apply to an identity and/or resource.
    Useful for troubleshooting conflicts / understanding why access has been granted - or not

18. Should be able to report on which policies/rules applied to an identity and/or resource at a specified
    point in time.
    Useful if there is a dispute over whether an individual had access to one or more systems

19. Should monitor usage to detect attacks on the system.
    Organisations have a legal duty to protect personal data.

4.3.4 Directory service

1. Must support LDAP.
   This is the industry standard

2. May use Active Directory
   Used to control access to resources in many organisations

3. May provide virtual directory.
   Provides flexibility in how data is made available

4. Must support standard object types used in FHE e.g. EduPerson
   Systems designed for the sector assume standard object types

5. Must provide access controls.
   There are many standard tools for connecting to LDAP directories, so access controls are essential
   to maintain privacy
6. Must limit data mining opportunities, especially for anonymous binds.  
   *Reduces the risk of data exposure*

**4.3.5 Groups service**

1. Should support dynamic groups  
   *Most efficient way of defining some groups*
2. Must support system maintained groups  
   *Many groups can be derived from existing business data*
3. Must support ad hoc groups  
   *Supports organisational flexibility by allowing individuals to be grouped to fit activities which cross team/departmental boundaries*
4. May support personal groups  
   *Allows informal associations which are often important to how organisations work*
5. Should support composite groups based on set operators: union, intersection, complement  
   *Provides flexibility in defining groups*
6. Must support searching for groups using internal and custom attributes  
   *There may be tens or hundreds of thousands of groups*
7. Should support inheritance of members when a group becomes a member of another group  
   *Makes managing groups easier*
8. Should allow clients to follow inheritance chains to determine how indirect memberships arose  
   *Useful for troubleshooting*
9. Must enumerate all groups for which an identity is a member  
   *Provides user-centric groups management*
10. Should support name spaces including searching and browsing by name space  
    *Provides structure and prevents name clashes*
11. Should support self-service groups with rules to govern who may opt in or out  
    *Allows individuals to subscribe to services*
12. May support membership expiry  
    *Provides flexibility, particularly when granting temporary access*
13. Should support site-specific attributes  
    *Useful for integration with local systems*
14. Must provide access controls to determine who can view/modify groups and memberships including changing access controls  
    *The existence and/or membership of some groups may be sensitive*
15. Must support access by / provisioning to external systems  
    *Ensures that group definitions and memberships are widely available, up-to-date and consistent*
16. Should support notifications to external systems when groups change  
    *Ensures group information is up-to-date*
17. Must support auditing and reporting as per other components  
    *Supports troubleshooting and misuse detection*
4.3.6 Asset repository

1. Must allow definition of arbitrary object types.
   *Supports flexibility as requirements and types of assets will change over time*

2. Must allow relationships between objects to be defined i.e. Printer x is in room y on the fourth floor of building z.
   *Allows flexibility in defining access rules and reporting*

3. Must allow assets to be associated with organizational units and other structures
   *Allows flexibility in defining access rules and reporting*

4.3.7 Provisioning

1. Should provide APIs to allow custom integrations including programming language/operating system neutral APIs
   *Facilitates integration and provides flexibility*

2. Must support robust and timely data synchronisation with a range of external systems
   *Required for an efficient system*

3. Should support message queues both for notifying external systems of changes and for receiving notification of changes from external systems
   *Provides flexibility and supports industry trends*

4.4 Generating Specific Institutional Requirements

In order to progress with work on Identity Management, it will be necessary to go from general requirements to ones which are specific to the institution wishing to carry out the work. This is essentially done by understanding the current situation regarding IdM, then deciding what needs to be changed and how best to carry out this change.

One important method to find out the current state of affairs is to carry out a comprehensive audit (or to customise a cut-down version of the audit to fit local requirements). Smaller scale exercises, such as discussions among stakeholders involved in the provision of the major IdM functions of the institution, or the use of surveys about satisfaction with the IT Services department's work. More information is given in the Gap Analysis section, which also discusses how to use this material to create an analysis of the work which needs to be done.

Business analysis and requirements analysis tools such as the development of user stories relating to IdM (from individuals such as developers seeking to integrate their work with central IdM, or IdM stakeholders in general), as used in agile development, and process modelling can be used. The assistance of a trained business analyst may well prove useful in this task. The lists of general and functional requirements appearing earlier in this section are likely to provide at least some requirements which are relevant to the specific situation being addressed by the work.

Whilst it is likely that those involved will have considerable experience in the development of requirements, it is worth bearing mind that they should:

- contain sufficient details that they can be implemented
- include measurable tests to check that they have been met by the implementation process
- include non-technical requirements as well as technical ones
- ensure that relevant procedures and documentation are produced
- ensure that security and privacy concerns are properly addressed

See also how to manage an IdM project below.
5 Discovering and Auditing Current Institutional Identity Management

5.1 Introduction

Executive Summary

This section details an important method which can be used to find the state of IdM in an institution: a comprehensive audit. This is a large scale method which endeavours to find all the important business processes within the institution which relate to the management of identity. It should cover the whole identity cycle from user registration to expiry, and its scope is wide enough to include small scale unofficial IdM, and non-IT based IdM, such as paper based access control lists for access to specific physical resources.

For FHE staff who might want to propose, organise, and carry out an audit, this section details:

- what is meant by an audit
- how to propose an audit to senior management
- how to project manage an audit
- how to find those who carry out IdM in an institution
- how to find out how IdM is carried out by these people
- how to analyse the information obtained by the audit
- how to present the information to senior management sponsoring the audit

The key results of the audit should feed into a gap analysis and the most important benefit is obtained through the use of the gap analysis to improve security and productivity in an institution through improvements in IdM processes.

Section contents:

- 5.1 Introduction: Describes what is meant by an Audit and why it is a useful exercise
- 5.2 Justifying an Audit to Senior Management: Describes a business case to support an IdM Audit
- 5.3 Phase 1: Preparing for the Audit: The tasks which should be carried out before an Audit can start.
- 5.4 Phase 2: Identity Management Discovery: How to discover who is carrying out IdM in an institution
- 5.5 Phase 3: Identity Management Investigation: Discovering what IdM tasks are carried out within the institution
- 5.6 Phase 4: Identity Management Analysis: Describing how to create a report based on the discoveries made in the Audit
- 5.7 Acknowledgements

5.1.1 What is an Audit?

A audit is a comprehensive, detailed study of an organisation's identity management systems. The aim is to find out how procedures relating to identity management are carried out, even if some of the practitioners do not realise they are identity managers.

The audit process described in this section describes a large scale project to discover as much as possible of an institution's IdM processes. This may not be considered an appropriate use of resources, though the
more that is known, the easier it is to find problems and plan to fix them. Smaller organisations, in particular, will not necessarily have to carry out such an elaborate process to obtain much useful information; the processes and requirements for IdM are likely to be simpler, and the resources less likely to be available. Thus, the material in this section is intended to be viewed as advisory rather than prescriptive, and should be freely adapted to local circumstances. Some suggestions of how the audit could be cut down if necessary are discussed later in this section.

5.1.2 Why Hold an Audit?
A more detailed business case for holding an identity audit is discussed in the next section. However, the essential reason for carrying out this process is that FHEIs are complex organisations, with many people likely to be carrying out identity management tasks (sometimes without actually realising that they do so), and where there are often processes which are poorly documented, designed by tradition rather than with considerations such as security in mind, or duplicated between departments and/or individuals. As technologies such as Federated Access which rely on accurate identity-related information being available become commonly used, it is important to ensure that identity management processes are streamlined, documented, secure and accurate. Many of today's business decisions (particularly relating to IT procurement) involve identity management as potential requirements or affected by the outcome, and a detailed understanding of existing identity management processes as provided by an audit will provide the necessary input for the decision making process.

5.1.3 The Limitations of an Audit
- An audit is not a survey. It is not designed to obtain quantitative results with measurable standard deviation as an opinion poll. The sample questioned in an audit is small, and carefully hand picked.
- The accuracy of some of the opinions obtained from interviewees is limited. Because of the nature of the sample, the answers to some questions will be coloured by greater knowledge of the identity management environment of the institution than a survey. (This is likely to lead, for example, to higher measures of satisfaction with the way that the institution manages personal data.)
- An audit does not measure actual behaviour, but interviewee's reports of their behaviour. This may make them less likely to admit to flaws in the processes and in how documented processes are carried out.

Other activities can be carried out in parallel with an audit to provide supplementary information of the sort that is listed here.

5.1.4 Customising a Smaller Scale Audit
There are two main reasons why an institution might want to consider cutting down the full audit process described in this section. There may not be sufficient resource to spend the time and effort which the full process requires, or the organisation might be of a nature where the full process is not appropriate - IdM processes in a smaller institution will be simpler, and some organisations may not carry out some of the functions being investigated (see for example the UK Data Archive's case study, which applied an audit of this type in a body which acts principally as a service provider).

There are two ways in which an audit could be cut down in scope. The first is simply to talk to fewer people, concentrating on the people involved in the core IdM processes. This runs the risk of missing important information, as issues to address are less likely to occur in these large scale, relatively well understood and centralised services dealing with the main categories of user than where people have invented their own procedures for ad hoc IdM, or where the individuals whose identity is being managed are unusual. However, there would be considerable time savings in the discovery phase of the Audit, as most of the individuals involved will be well known and probably key people within departments such as SIS or Computer Services. Interviewing fewer people will also make the investigation stage easier and there will be less material to interpret for the analysis stage. Effectively, this approach would make the Audit a series of meetings with a representative group of stakeholders, as identified by the Key Researcher. Such an approach requires considerable knowledge of the existing state of official IdM practices at the institution.

The second way to cut down an audit would be to concentrate on a specific gap which is likely to occur. (The Gap Analysis section includes a discussion of the major gaps which commonly occur in FHE Identity
5.1.5 Summary of Audit Process

We start by giving a broad outline, to put the details discussed in the following four sections into context. The work required for an audit divides naturally into four phases, first preparation, then successively IdM discovery, investigation and analysis. It is important to realise that all the details are intended as guidance rather than to be as strict rules, to allow for adaptation to the culture of the institution carrying out the audit. In many cases, more suggestions will be given than are practical, so choices will need to be made.

The preparation phase consists of finding an appropriate individual to take on the role we have designated "key researcher" (abbreviated KR), and ensuring that they have the knowledge required to carry out the audit (such as sufficient technical understanding to engage experts in the configuration and use of complex software). The KR will need to plan the process, looking at the various options suggested here and adapting this process to the local institutional culture, as well as establishing a timetable for the audit. Overview of the process (by an appropriate group, e.g. an IT Manager's Forum, and backed up by a senior member of the institution) is also set up in this phase.

The IdM discovery phase aims to find as many individuals as possible within the institution who may carry out duties which amount to identity management. From these identified individuals, a target list of those to be interviewed needs to be selected, and then interviews scheduled. A parallel process of documentation discovery should be carried out at the same time.

The IdM investigation phase contains the interviews themselves, and the basic writing up of the information gathered this way. This guide discusses several methods for carrying out this process, with the key aim of making the next phase as easy as possible.

The final phase, the IdM analysis phase, aims to produce a coherent report out of the materials that have been gathered, with a description of the institution's current identity management regime and recommendations for consideration by senior management.

5.2 Justifying an Audit to Senior Management

In order to carry out an audit, the senior management at an institution will need to be persuaded that it is a useful exercise, and will provide more benefit than the cost of the work. However, it is not easy to provide a single business case which can be applied to each FHEI, because each institution is different, and each has slightly different priorities for carrying out an audit. Thus, we give a basic template which can be adapted by an individual or team who wishes to propose an audit to their institution, or make the initial steps towards project managing an audit. In particular, no detailed costings are given, as these would quickly be outdated and will differ for different institutions in any case.

5.2.1 Generic IdM Audit Business Case Template

This is based on the summary of business case structure provided by the Office of Government Commerce (no longer available).

**Strategic Fit**

Reference to the identification of Identity Management as part of any existing institutional strategic plans.

**Business Need**

The business need for an audit has been covered in more detail elsewhere in this Toolkit. However, it is worth summarising the points which are likely to need to be included to show the business need for an audit. Firstly, there is a need for high quality Identity Management.

- Institutions increasingly have legal constraints which regulate aspects of Identity Management (including general legal requirements such as the Data Protection Act, and requirements from
agreements the institution has entered into such as license agreements, federation membership
agreements)

• Institutions have a duty to their members (staff, students) to manage data about them competently,
and security breaches will damage the reputation of the institution

• Inefficient, poorly documented and duplicated business processes may be an unnecessary financial
cost to the institution

However, FHEIs are large and complex organisations. It is not possible to ensure that its Identity
Management is of sufficiently high quality or to plan for improvements without an understanding of the
processes currently being carried out across the whole institution. No one individual will understand the
global picture unless this has been surveyed across the organisation, which means that an audit is
necessary for Identity Management planning. This need can be addressed by an audit of the Identity
Management processes as described in this Toolkit.

Organisational overview

This section should contain the following information (quoted directly):

• Describe the organisation's main aims, organisational structure and key responsibilities.

• Describe the main aspects of the business strategy: strategic vision, strategic plan and continuing
aims.

• Outline the main themes of the IT or estates strategy, where relevant (such as delivering information
electronically to the public), key programmes and projects.

The details here will vary from institution to institution. It is good practice to reference and quote from
documents already in existence in the organisation, and this Toolkit will therefore not offer generalised
versions of this material.

Contribution to key objectives

The business strategy and the IT/estates strategies identified in the previous section are likely to include
targets, objectives and so on. The business case for an IdM audit needs to point explicitly to those
targets/objectives which it will help to achieve. Again, this Toolkit cannot offer generalised guidance here, but
it should be borne in mind that an audit may not directly relate to objectives which will be made easier to
achieve by carrying one out, for reasons mentioned above as the case for high quality IdM.

Stakeholders

The following groups are likely to be stakeholders in an audit and its outcomes in any institution. When
putting together the business case, the author needs to consider whether other groups in the institution
should also be included, to reflect unique properties of the institution; the listed types of stakeholders may
well also require local modification.

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Interest</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Managers</td>
<td>Oversight of most of the institution's major, centralised IdM processes</td>
<td>High</td>
</tr>
<tr>
<td>Library staff</td>
<td>Access to electronic resources is one of the important ways in which identities are exposed beyond the institution</td>
<td>High</td>
</tr>
<tr>
<td>Staff in MIS, Registry, Human Resources and similar administrative departments</td>
<td>Oversight of much of the raw data managed by IdM processes</td>
<td>High</td>
</tr>
<tr>
<td>Senior management</td>
<td>Overall responsibility for IdM and public accountability for security/privacy lapses</td>
<td>Medium</td>
</tr>
<tr>
<td>Other staff and students /</td>
<td>Security and privacy in the handling of their personal data</td>
<td>Low</td>
</tr>
</tbody>
</table>
### Existing Arrangements

This section in most business cases is intended to give an overview of the systems which will be affected (replaced, or differently integrated) by the proposal if carried out. The current IdM processes are precisely what an audit is intended to find, so this information will not be available when the business case is compiled. The reasons why an audit is necessary to do this are covered in the Business Need section above.

### Scope

An audit as described in this document is a large scale procedure. It may be possible to consider a cut down version of an audit, which would answer some of the questions which a full scale one would be intended to cover. However, such a minimised audit would be more likely to miss important aspects of IdM in the organisation, which means that associated risks would be considerably greater. (Exactly how an audit could be cut down would depend on the institution.) Similarly, it would be possible to set up a larger scale audit, which could (for example) elicit information from a larger sample of end users. The risk here is that the IdM environment might well change too quickly for such an audit to capture it in a timely manner.

### Constraints

Again, the information here will depend on the individual institution. However, constraints are likely to include:

- reluctance of identity managers and middle management to reveal potentially embarrassing information about IdM problems
- availability of an individual to act as Key Researcher for the audit, and the need to appoint someone to cover for the time spent carrying out the audit

### Dependencies

There are unlikely to be any.

### Strategic benefits

The major benefit is that a clear understanding of the local IdM culture will make it possible for future projects with an IdM component to be properly planned, rather than relying on unfounded assumptions as to how IdM is carried out. Specific benefits will all be ways in which this will work in detail. In particular, the audit should measure gaps between current practice and regulatory requirements which will enable the institution undertake the change needed to better meet these requirements in future.

### Strategic risks

The crucial risks in an audit are connected to the key researcher. An appropriate individual (see below) should be provisionally selected before completion of the business report, so that it becomes easier to assess the risk of:

1. Non-availability of the researcher. Replacing a researcher part way through an audit - a process which will take around a year - is going to be extremely difficult.
2. Difficulty finding a replacement to cover the researcher's normal duties. The time spent on the audit is likely to need to be covered, and if the individual chosen is hard to replace, their management might well feel that they should add the audit to their existing duties, which makes it much harder for them to carry out the audit successfully.
3. Difficulty in accessing required information. This can be ameliorated in several ways, including prior agreement on scope, methods, etc. between the researcher and other staff involved (an oversight committee, as described in detail below, is important for this); prior commitment of senior staff; sensible planning of timetable (to avoid busy periods for staff likely to be involved as interviewees, again discussed below).

4. Non-availability of interviewees. This risk is discussed in more detail below, and arises from such issues as busy schedules and annual leave. Amelioration should come from planning the audit so that the information gathering phase does not take place wholly during peak leave time periods (generally, Christmas, Easter and August – though for some staff, such times might be the best times to make space to be interviewed), the involvement of management in the audit process, and a willingness on the part of the KR to re-schedule.

**Critical success factors**

The success of an audit is seen by the timely production of a report, signed off by the audit oversight committee, with recommendations for improving IdM in the institution.

**Options appraisal**

The options for an audit are described in more detail in the audit plan section of the Toolkit. However, key options which should be discussed include:

- constitution of oversight committee
- audit scope
- any important local differences which need to be covered
- whether other IdM assessment activities should be carried out in parallel (e.g. assessment of user knowledge of identity security)

There may be opportunities to work as part of a consortium carrying out parallel audits, which is something which can greatly aid the researchers at each institution through mutual support. Useful places to find appropriate contacts that might be able to arrange this include the Identity-Project-Public mailing list.

The audit planning page includes a suggested timetable, which can be adapted to provide a range of delivery options for the audit.

**Commercial aspects**

The aspects of the business case listed under this heading are not relevant here.

**Affordability**

Budget costs are discussed in the audit plan. The major cost, the appointment of cover for the key researcher (about 12 months at 0.2 FTE), will depend on local circumstances and the choice of researcher.

**Achievability**

(This is very much a matter for local assessment.)

**Similar Projects**

A variety of institutions carried out audits as part of The Identity Project (website no longer available); audits were also carried out as part of the road test of this Toolkit, and several of the Case Studies for the Toolkit involve versions of the Audit process. For direct contact with institutions which have carried out an audit, email jiscinfonet@northumbria.ac.uk.

Project roles
These are discussed in some detail below.

Procurement Strategy
Not applicable.

Project Plan
The audit is quite a simple project, and the timetable has already been discussed in outline.

Contract Management
Not applicable.

Risk Management Strategy
This is discussed below in the audit planning section.

Benefits Realisation Plan
Not applicable.

PIR/s and PER
Post Implementation Reviews are not applicable to the audit. The oversight committee, in signing off the audit report, should be able to produce a short Project Evaluation Review.

Contingency Plan
Not applicable.

5.3 Phase 1: Preparing for the Audit

5.3.1 Involvement of Senior Staff
It is vital for an audit to have the backing of senior staff at the institution, because:

1. Without it, there is a high risk that the audit will go nowhere: the final report will identify shortcomings, and backing from senior staff will help ensure that the report conclusions can be acted upon. A major disadvantage of using an internal KR (as recommended below) is that their report may be given less credence in some quarters than one produced by an independent external consultant, and senior management will need to be willing to support the credibility of the audit. The audit is likely to identify gaps in both strategy/policy and technical implementation, and without senior management involvement, it will be difficult to resolve and address high level policy issues.

2. Without it, the KR will find it difficult to persuade other members of the institution to discuss sensitive material relating to IdM.

3. It is likely that a fairly senior manager will be needed to be involved in the process of funding and recruiting cover for the time spent by the KR on the audit.

The senior figure should be someone at director level. The library and/or IT Services director would be an appropriate choice. This individual will have the final responsibility for the audit (e.g. taking it forward to central planning committees, and overseeing work using the results to improve institutional IdM), and will be invaluable as support for the KR to give them added credibility. This will be crucial in phases 3 and 4 of the audit, as detailed below. The final task for this member of staff will be to sign off the final report produced by the KR, which again will give the results of the audit credibility within the institution.
5.3.2 Appointing a Key Researcher

It is essential for the audit to be the responsibility of a single individual, even if parts of the work are delegated to others. It is also essential that they be familiar with the organisation's culture, and it engenders trust in interviewees if the interviewer is also from the institution.

This means that an existing staff member needs to be seconded from their normal duties for the period of the audit process. It is estimated from experience carrying out similar audits that a total of 300-350 person-hours is likely to be the approximate amount of KR staff time required to carry out an audit, which amounts to approximately 0.2 FTE over twelve months (taking holidays into account). Twelve months provides a reasonable timetable for the audit as discussed below. It is advisable to find a replacement for the time spent by the KR on the project, rather than expecting the KR to fulfil their usual duties alongside the additional work required for the audit. However, it is realised that this advice can be difficult to follow in reality.

Suitable potential KRs include members of IT departments, librarians and graduate students. Requisite experience and skills include experience of business analysis, a certain amount of technical knowledge and the confidence that they will be able to carry out interviews comfortably. The following paragraph summarises the skills and experience needed as they might appear in a job advertisement:

"You will be a graduate or equivalent with experience of survey methodology, undertaking information gathering by questionnaires and interviews. A high level of competence as a user of IT is required. You will be able to communicate effectively with a wide range of academic and support staff as well as external organisations and individuals and have the ability to translate key technical issues into non-specialist language. You will have initiative and enthusiasm, excellent written communication skills and well-developed analytical skills. Experience of writing reports would be an advantage."

5.3.3 Audit Governance

In addition to the backing of a senior figure, there needs to be some infrastructure to manage the audit as a project. It is strongly recommended that any institution carrying out an audit should establish (or identify an existing institutional body that can act as) a local project advisory group (AG), representing key departments or services of their institution concerned with Identity Management. The AG will provide local advice to the project and help to raise local awareness of the issues with which it is dealing.

Existing bodies are likely to work better as an AG than ones convened for the purpose, since the audit will then be an additional item on the agenda at an meetings already arranged, rather than a new meeting that needs to be fitted into busy schedules. An appropriate forum should include members who have some technical knowledge, but should not be too heavily IT focused (because then the audit itself is likely to become biased in that direction). A suitable existing body might be an IT managers committee, as management roles should enable members to look beyond IT issues. This body should, at least for the duration of the audit, either include the KR and their line manager or permit them to attend meetings to discuss the progress of the audit.

Meetings of the AG which discuss the audit should occur at least at the transition points between each phase (approximately), to review the phase coming to an end and help the KR make detailed plans for the phase about to start. Ideally, a meeting in the central point of each phase would help the AG keep the process on track. The final task of the AG would be to approve the audit report to be passed to the senior figure backing the audit for endorsement, and commit to using it as part of their future planning.

Before any planning can be done, it is essential for the AG to agree on what they mean by the term "Identity Management". The definition of Identity Management in this Toolkit should be used as a starting point for discussion. For many, the meaning of the term is restricted to account provisioning, or access management, which gives it a distinctly technological bias. However, a large part of the audit process described here deals with the investigation of business processes which deal with a much wider picture of IdM, and which in particular include "informal" processes which are not part of official procedures. These business processes may well involve technology but do not have to; for example, a requirement that new students prove their identity on registration with a passport verified by a human being is part of IdM but does not use computers (except possibly to indicate in a database that the identity is considered proven). This agreement is essential to avoid differences between the KR and AG about the scope of the audit.

The second management decision to be made before starting is how long the audit should take. The 350 or so working hours for the KR can be spread over anything from about three months to a year (any longer and
it is likely that the information being audited will change faster than the audit discovers it). However, the
demands of interview scheduling and the KR's other duties are likely to mean that a timescale nearer the
upper than lower limit is going to be sensible, from nine months to a year. This time should be organised in
such a way that busy periods in both the KR and potential interviewee schedules do not coincide with
intensive parts of the audit schedule. Busy periods are obviously likely to be the time including and around
student exams (for teaching staff, students and administrators involved in the exam process) and the period
of applicant clearing and the student enrolment period at the beginning of the academic year (for many
administrative staff, as this period involves a considerable percentage of the year's identity management
work).

The timetable for the audit would divide phases 2-4 into equal periods, with phase 1 being somewhat shorter
(considering the timetable to start from the appointment of the KR). A possible 11 month schedule could then
run as follows:

<table>
<thead>
<tr>
<th>Phase</th>
<th>Start</th>
<th>End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td>1 November</td>
<td>31 December</td>
</tr>
<tr>
<td>Phase 2</td>
<td>1 January</td>
<td>31 March</td>
</tr>
<tr>
<td>Phase 3</td>
<td>1 April</td>
<td>30 June</td>
</tr>
<tr>
<td>Phase 4</td>
<td>1 July</td>
<td>30 September</td>
</tr>
</tbody>
</table>

With this timetable, Phase 3 would be the most problematic, and it would almost certainly need to be allowed
to start earlier and finish later, catering for interviewees with student exam responsibilities.

Among the other decisions that need to be made about the report that should be delivered from an audit, is
that of publication. Will the report be entirely public, or mostly public with some restricted access parts, or
generally circulated internally within the institution, or only circulated within a small group? This decision will
depend on the institutional culture, and also on how high a standard of identity management the institution
perceives itself to have reached before the audit takes place. Where the report or parts of the report are used
as the basis for work following on for the audit, there may be requirements (e.g. from funding bodies) that
this information is public.

The KR is likely to have to carry out tasks new to them during the audit, whatever their background. A group
of institutions might therefore benefit from carrying out parallel audits as a consortium, so that KRs can give
each other mutual support. At the very least, a diversity of backgrounds should be represented on the AG.

5.3.4 Preparation for the Audit

There are two important tasks which need to be carried out before the audit proper can begin.

**Understanding IdM**

Firstly, the KR needs to have a certain level of familiarity with the technical issues which they will be
discussing with the interviewees. This knowledge does not have to be deep, just sufficient that the interviews
are not spent explaining what, to the interviewees, are basic concepts: the KR should not need to ask
questions such as "What is LDAP?". Equally, the KR cannot let issues they don't understand be ignored, at
the risk of producing a report which is full of technical errors that reduce its credibility. The list of topics in the
Toolkit glossary should give a good idea of what the KR needs to know: anything that prompts a query in the
mind of the KR is worth reading more about to get an idea of the topic and the issues to be addressed in an
interview with an expert on that topic.

A quick visit to a search engine should provide simple primers on most of these subjects, where there is not
information already in this Toolkit. Alternatively, members of the AG should either be able to explain or know
who on their team could explain areas which are not known to the KR.
**Audit Project Plan**

It is sensible in general and likely to be a requirement from institutions carrying out an audit that the KR produces a detailed project plan for the audit as it is to be carried out for the particular institution involved. Such a project plan will expand on a local business case, and will draw on the material throughout this section (in particular, when devising a detailed timetable).

Institutions may have internal requirements for the production of project plans, but in the absence of these, suggested headings for a project plan include

- **Background** Explaining what the audit is, and how it will be carried out in general terms.
- **Aims and Objectives** What should be achieved by the audit, preferably including targets (e.g. for number of interviews).
- **Outputs** A brief description of the final report, and how it will be published and used after the audit is complete.
- **Stakeholders** This should match the information in the business plan.
- **Risks** This should match the information in the business plan.
- **Detailed timetable**
- **Personnel** Some information about the qualification of the KR for the task.

A simple sample MS Project Format Plan for an IdM audit is provided in the online Toolkit\(^\text{14}\) to help with the production of the plan. The task breakdown as a GANTT chart for this plan can also be seen there\(^\text{15}\). (This plan is illustrative only, and not intended to be prescriptive.) This plan contains tasks assigned to a role which has not yet been mentioned, the Audit Manager. This role was created specifically that tasks to be carried out before the work of the KR begins could be assigned, and this is likely to be the proposer of the audit or the line manager of the KR, or both (if these are different people).

As part of the planning for the audit, the KR will have to decide how to organise the interview material so that writing the report is as simple as possible. For the audits in the Identity Project, a WIKI with tagging was used, so that it was possible to collect together all the interviews which mentioned (e.g.) certificates or student records. This approach illustrates why organisation is necessary, though it is a rather heavyweight approach for a single audit not part of a collaborative project. The important point of whatever organisational method is chosen is to be able to quickly retrieve those interviews and published documents which are relevant to a particular section of report, to be able to know which audio files are full records of the interview which has notes that a not as clear as they appeared to be, and so on. Any sensible method to do this (such as a master document which records the interviews by subject matter) should be acceptable, provided that it is adhered to consistently throughout the audit process by the KR. Since information provided might include handwritten diagrams, the KR should ensure that they have access to a scanner in case one is needed.

### 5.3.5 Checklist

By the completion of this phase, the following should be in place:

- a member of senior management backing the audit
- a committee which will oversee the audit and who have a broad agreement on what IdM means and on the aims and methods of the audit
- a key researcher who is:
- freed up from existing commitments for the time they will spend on the audit
- familiar with sufficient technical detail of IdM to understand the answers they will get in interviews
- a timetable (and probably a project plan) for the audit

---

\(^\text{14}\) [https://identitymanagementinfokit.pbworks.com/w/file/51839805/IDM_Readiness_Audit_Gantt_Chart_(MS_Project)_Version2.mpp](https://identitymanagementinfokit.pbworks.com/w/file/51839805/IDM_Readiness_Audit_Gantt_Chart_(MS_Project)_Version2.mpp)

\(^\text{15}\) [https://identitymanagementinfokit.pbworks.com/w/file/51839804/IDM_Readiness_Audit_Gantt_Chart_Ver sion2.pdf](https://identitymanagementinfokit.pbworks.com/w/file/51839804/IDM_Readiness_Audit_Gantt_Chart_V ersion2.pdf)
• a plan for the organisation of material discovered in the audit, and the technical apparatus required for this (e.g. a WIKI and access to a scanner)

5.4 Phase 2: Identity Management Discovery

Before finding those who perform identity management, the KR will need to decide what is in scope and what should be ignored. Several examples of boundary cases are given in this section, and whether or not they are considered in or out of scope will depend on the resources available, and whether a particular case is of special importance to the institution carrying out the audit. The commentary is based on the definition given in Section 2 of IdM, which should be one of the criteria considered when deciding whether an activity is in scope.

Activities of members of the public (e.g. descriptions of which parts of campus buildings can be accessed without any identity check) are not truly part of identity management. For this a member of the public is defined as “An individual with no relationship with an institution which results in their identity becoming known and managed by that institution for purposes of access.” This means that a member of the public who registers as a library visitor in order to use collections for reference, for example, is no longer classed as a member of the public and the management of such users is identity management. However, the KR and AG may decide that analysis of how controls are used to prevent members of the public having access that is intended to be restricted to identity managed individuals is something that their audit needs to cover.

Lists of individuals maintained for contact purposes only (e.g. marketing lists, “Friends of”...) may not be considered identity management, because these lists are not used for a purpose connected with providing access to a resource. However, such lists may well interact with other systems (such as alumni databases), and this interaction may be considered within scope.

Paper-based IdM is not considered an out of scope technology, and where processes analysed by the KR involve the use of paper, this should be noted. However, it may not be worth the time to search minor paper-based IdM: it is probably used in many relatively informal or short lived contexts that will be hard to discover, classify, and may not be meaningful in the context of an audit aiming to make recommendations to an institution for the long term. For example, a member of staff might write down a list of external visitors on a list given to security guards who then let them in for a meeting; such processes are often hard to find, and not generally worth trying to formalise. They may also be electronic; email could be used instead of a paper list in the suggested example. This would not then make the process worth examining in detail.

There is also the question of informal IdM, particularly services which go beyond standard institutional boundaries such as Facebook\textsuperscript{16}. This is likely to be too big for proper investigation as part of the audit, especially as the institution will have little official role in their management (e.g. Facebook groups which appear to be associated with the institution are unlikely at the time of writing to be managed by an individual paid to do so by the institution). Looking at institutional policy on such services may be in scope. Anything that does not interact with the business processes of the institution is likely to be considered out of scope for practical reasons.

5.4.1 Discovering Identity Managers

The major method used by the audit to discover what IdM is carried out at an institution is through interviews with individuals who are either identity managers themselves (though they may not in fact realise this) or who are representative end users. The first major task of the audit, the most important part of the second phase, is to discover which members of the institution actually act as identity managers.

It is important to interview end users of IdM, as well as practitioners. To this end, interviews should also be organised with sample members of academic staff, administrative staff and students. (Time constraints will mean that the sample tends to be selected from individuals already known to the researcher, which will make it unrepresentative but not necessarily in an unhelpful way: they are more likely to co-operate with the KR, apart from anything else.) More representative views from users should be obtained by other methods.

Three major methods are suggested for obtaining lists of appropriate contacts. The culture of the institution carrying out the audit and, in some cases, the usual work of the KR, will mean that some of these methods work better than others. It is advisable to try at least two of them, particularly as they are aimed at finding individuals who carry out different types of IdM. Some suggestions on the content of contact emails or phone calls are given below.

\textsuperscript{16} \url{http://www.facebook.com/}
The outcome of this process will almost certainly a lengthy list of contacts, possibly up to 100, and so the list will need to be prioritised as discussed later.

**Organisational units**

Obtaining a list of institutional organisational units, and contacting those which seem likely to perform some IdM function. Lists that can be used for this purpose include institutional telephone directories, and directory pages or departmental listings on the institutional web site. The contacted individuals from such a list should either be ones whose job titles suggest an IdM function, or ones which are designated as first contact points. This finds the units which are major stakeholders in IdM in the institution, but is not able to discover small scale and informal IdM. Names used for the organisational units within UK FHEIs vary considerably, but the following list of "core functions" should provide a useful checklist of the minimum expected set of departments which perform IdM.

- student record system
- human resources / personnel
- email/network account provisioning
- management physical access to buildings (potentially both access cards and security/reception)
- management of library resource access (both physical and electronic resources)
- VLE and/or portal management
- alumni records / development office
- finance/payroll

This list is deliberately slightly vague, to cope with differences in organisation. Not only are many of these functions named differently by institutions, but several of them may be aggregated with others or split between departments. Every institution has a Data Protection Officer, and they will know enough about the IdM which is going on in the institution to be considered a core individual for the KR to interview.

The KR should think about use cases where IdM is obviously needed (e.g. what happens when new PhD students arrive) - both what is meant to happen and what actually does happen; this can help find gaps in such lists which are specific to how a particular institution operates. For example, each user of the institution's services has a life cycle (first contact, access granted, updates to personal information etc., final contact, expiry of access rights) and consideration of this for a variety of users may highlight IdM which is likely to be happening which has not yet been discovered. As a check towards the end of the audit, the KR should be able to draw diagrams indicating how these obvious processes are broken down and handled within their institution from the information they have gathered.

**Known contacts**

Directly contacting those known to the KR who are likely to be involved in IdM. This may include individuals who are "end-users" of the institution's identity management systems (such as students) who do not carry out management functions themselves but may well have opinions on the way the institution does so and, of particular interest, may have different opinions about how this works from those who do carry out such management.

Known contacts are also likely sources of other names to contact. Many of them will be in positions to know about systems which manage identity; for example, the Data Protection Officer is likely to know about the use of sensitive data in the institution.

**Global message**

Sending a global message to every staff member in the institution. Using existing channels (email lists and electronic noticeboards) to send a generic message supplements the first two methods by finding samples of the small scale and informal IdM, but it may fail to find everything (a lowish response rate, and no responses from some of those identified from the first two methods may occur, the latter possibly due to these individuals having already been contacted, or expecting to be contacted anyway).

With this method, it is particularly important to word the contact email so that
• it is clear that it is official and has the backing of senior staff of the institution
• it is very non-technical in nature, to find individuals who may not even know what identity management is

An additional important point is that the email should not be sent in a way which irritates either the institution's authorities, or its recipients. In particular, the KR should follow any rules and guidelines laid down for emails which go to all staff (which may, for example, require text to be included in weekly or monthly newsletters).

Other methods

• Make direct contact with departmental secretaries/IT administrators who might well know of local, informal IdM.
• Find people who don't fall into standard roles, and contact those who organise their access to institutional resources. Examples of such people include visiting academics, honorary staff, contract cleaners, summer school students, conference guests, emeritus professors, IT and other technical contractors, students housed away from main campus, or library visiting users.

Suggestions for content

People do not necessarily all mean the same things when they talk about identity management, and it is important to be clear, particularly when addressing users who may never have heard the term or considered applying it to their work. The following questions are suggested as giving individuals who may never have heard the term an idea of the purpose of the audit, and whether their input will be relevant. The notes are given to indicate why they might be less useful in isolation than when used together.

• "Do you ask anyone to prove who they are?" Advantage: completely non-technical. Disadvantage: Includes people who apply identity management without actually managing it, such as security guards.
• "Do you maintain information about individuals which is used by them to gain access to (physical or electronic) resources?" Advantage: Restricts "yes" answers to people who really do identity management, pretty much. Disadvantage: "maintain information" is rather vague - responders may what sort of information is meant, though most kinds would be relevant to an audit.

See also Wikipedia's Identity Management article17 for other ways in which the subject is explained non-technically; this might well be a useful reference to include in initial emails.

Any emails which are sent out to staff by a KR will need to be customised to fit the institution's culture. The KR will also need to find out if there are accepted ways in which this should be done (e.g. periodic email newsletters); it may be the case that there are non-email based methods which are preferable (e.g. web servers used as noticeboards, or analogue mechanisms). We give here two example emails (based on those sent out by KR's on the Identity Project), which should help with drafting such material. The first email included the questions above after the introductory text quoted below, and is aimed at individuals found through the analysis of organisational units, while the second email has the questions incorporated into the body of the email itself and was sent to all staff members.

It may be questioned whether "audit" was the best term to use when contacting individuals who might potentially be interviewees, as it carries associations that may not be entirely positive even if the process defined here is not intended to be negative. Alternative terms suggested include "review" and "inventory", but the best alternative is to use "research" wherever possible, because of its association with the normal practice of an FHEI.

Dear Colleague

I am writing to you to ask you to participate in an internal audit we are doing of identity management here at the University/College of X. I would appreciate it if you would direct this request to the relevant individual or individuals in your department or section responsible for this. This audit is part of a process defined in the JISC Identity Management Toolkit, and will be used to improve the management of users at the University. The result of this research will be a report.

completed by October 2010.

The questions set out in this email are designed for two purposes. First, to gain a general sense of who is responsible for identity management in each department or section and what steps are being taken across the University at both a formal and informal level. This would include both the official directives and guidelines set out and the actual processes that occur. This process will continue until May. Second, to identify and invite specific individuals for interviews to discuss their role and involvement in identity management in more detail. This process is scheduled to take place between May and July.

The concept of identity management used by this audit is classified widely and consists of forms of credential management (e.g. user registration and expiry procedures), handling data about University users (i.e. staff, students and non-University registered individuals) alongside security and privacy issues.

Because of the sensitivity of the issues involved in this project, all responses and interviews by individuals will be presented anonymously in the final report.

Thank you for your assistance in this matter. Should you have any queries about the questions in this email or the audit more generally, please do not hesitate to contact me.

Yours sincerely

Dear Colleague,

The Y University/College is carrying out an official audit of its identity management practices, based on the process defined in the JISC Identity Management Toolkit. This will be used to improve these practices, and help the University improve security and privacy for our users.

The purpose of this email is to find out those staff here at Y University/College who are involved in identity management (perhaps without thinking about their job in those terms) in the course of their work; and to get those who are to make themselves known to us.

There are many “identity management” procedures and systems at YU/C, formal and informal, electronic and paper-based. As well as central systems such as the door cards or the student information system, there are others run by departments or groups within departments.

There are 2 questions which can help to determine if you are in this category:
1. In the course of your work, do you ask anyone to prove who they are?
2. Do you maintain information about individuals which is used by them to gain access to physical or electronic resources?

If you answer "yes" to either of these questions please reply to this email, ideally with a brief description of the context in which you are working with identity management. Once we have a list of staff involved in identity management, we will follow up with a more detailed set of questions, either by email or possibly face to face meetings.

More information about the JISC Identity Management Toolkit can be found at: www.identity-project.org

Your responses will be helpful in planning future Y University/College identity management systems in order to enable interoperability with external services such as the UK Access Management Federation (http://ukfederation.org.uk) and to promote national and international collaboration with other institutions.

Many thanks for your time.

The essential points to get into such an email are the following:

- who you are
• why this is an official request not some random email from a person some of the recipients have probably never met
• how the recipient might identify themselves as an Identity Manager
• what they are being asked to do
• what is the purpose of what they are being asked to do
• some idea of the benefits to the individual and/or the institution of participation

5.4.2 Discovering Identity Management Documentation

Many of the discussions of good practice in identity management stress the importance of using documented procedures, both in normal operation and for resolution of problems. For example, it plays a major part in many of the requirements of ISO 27002 (formerly 17799)\(^\text{18}\), which deals with data security. Therefore it is essential that part of the audit should aim to discover as much documentation as possible, whether public or not, and whether aimed at administrators or end-users of systems.

The documentation to be found should generally ignore that delivered as part of a software package or other solution by a vendor, as this will usually describe all the different ways in which it can be set up and configured, whereas the audit is interested in the specific processes in use at an institution. Examples of the types of documentation an audit should find include leaflets for end users on how to apply for access to a specific restricted resource, such as the National Grid Service, and an unpublished description of how email accounts are provisioned produced by a leaving member of IT staff for the person who will take over their post.

As with the discovery of identity managers discussed above, there are several methods which can be used for this.

• checking appropriate pages from the institution's website and intranet (e.g. the pages for IT Services or student admissions)
• asking those interviewed whether there is documentation for the systems they work with
• looking in places where paper documentation is made available (e.g. the IT help desk)

It is to be expected that most people who are likely to know about official documentation will be interviewed, including the Data Protection Officer, who should have a good idea about the state of documentation across the institution.

When documentation is collected, it will be important to discover its status for publication. There may well be draft documentation which is not yet published which differs from that currently available to end users; there may be papers which are kept secret within a department because they would permit breaches of security (e.g. disaster recovery plans with lists of root passwords). The KR must ensure that any requirements of secrecy are followed, and be willing to give assurances to this effect when requesting copies of documentation. The KR should bear in mind that part of the recommendations of the audit could be to make some of this documentation more easily availability.

Gathering documentation might well also reveal individuals who are potential interview candidates (e.g. authors and maintainers, or those identified by the document as having responsibility for parts of a system involving identity management). Thus, while this process and the process of discovering interviewees take place at the same time, one may well inform the other.

5.4.3 Checklist

By the completion of this phase, the following should be ready:

• A long list of contacts who have some connection with IdM ready for prioritisation
• A list of the IdM documentation that has been found so far

\(^{18}\) [http://www.27000.org/](http://www.27000.org/)
5.5 Phase 3: Identity Management Investigation

In this phase, the contacts made in Phase 2 are prioritised, and interviews are arranged with those that the KR feels will be important or representative contributors to the institution's IdM. Scheduled interviews are carried out and written up.

5.5.1 Prioritising Contacts

The processes outlined in Phase 2 are likely to produce a lengthy list of potential Identity Managers. This list will need to be prioritised, to ensure that the time of the KR and the interviewees is usefully spent. It should immediately be possible to eliminate individuals whose IdM is trivial, or out of scope. There will also be some contacts whose function is duplicated by others (though this itself may be important); generally, only one needs to be interviewed, though in some cases interviewing several with similar functions may be useful (possibly with a joint interview) particularly if one interviewee can provide a management perspective and another the technical perspective, but neither is able to provide both. There will be contacts who it will not be necessary to interview, but whose role appears to include some interest for the audit; these individuals can be asked a short set of questions by email.

The core functions which need to be addressed by an audit are listed earlier in this section. Interviews will need to be scheduled with individuals who are involved with IdM for each of these functions, together with classes of end-user, who need to be interviewed as “consumers” of IdM in the institution. At least three classes of end-user need to be represented, including:

- a student
- an academic staff member
- an administrative staff member

Apart from these obvious targets, priority should be given to individuals who are unusual in some way. Higher education institutions are not all alike, and there may well be identity management functions or issues associated with the things that make an institution unique. These could include large scale involvement in the National Health Service; higher proportions than average of overseas students, part-time students, or other categories of students/staff (as documented by HESA19). It would almost certainly be possible to give similar distinguishing marks for any UK higher education institution. Since these unique characteristics are areas which may well not be well catered for by off-the-shelf IT solutions (whether these solutions are identity management products or not), looking at potential IdM associated with them is of high importance.

It is likely that cross-institutional initiatives will provide particularly interesting IdM problems and solutions, especially if they go beyond national frontiers. Such initiatives as the University of London External Programme20 or the way that the University of London central divisions act as service providers for the students and academic faculty of the federal university, are good examples of the type of initiatives which should be investigated.

5.5.2 Arranging Interviews

Issues which come up when arranging the interviews are mainly concerned with communication with a potential interviewee; in particular, what should be said about the interview itself, and how to try to arrange an interview with a reluctant interviewee.

While the request for an interview will need to be custom made for each institution carrying out an audit, there are several points to bear in mind when creating a request text. If the contact is not one who would have received a global message, then the considerations mentioned above for the content of such a message will apply here too. If they will have received a global message, then the invitation to an interview should repeat this as little as possible.

Apart from the information that may need to be included for this reason, an invitation needs to include:

- reminder of the audit’s existence, possibly including the information that it is supported by senior figures in the institution (though the KR may judge that this latter reminder may be best kept for a follow-up if such is required)

19 [http://www.hesa.ac.uk/](http://www.hesa.ac.uk/)
20 [http://www.londonexternal.ac.uk/](http://www.londonexternal.ac.uk/)

63 of 123
Here is a sample text. It has four alternative middle sections, depending on the relationship that the individual being invited has to identity management at the institution.

<table>
<thead>
<tr>
<th>Opening</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dear Colleague</td>
</tr>
<tr>
<td>The College of X is currently carrying out research to look into the way it manages personal identity for its users in order to improve services and to produce recommendations on best practice to ensure it meets its legal obligations in this area. The research will carry out interviews with a number of individuals over the next couple of months. The findings will feed into a case study report on the way identity issues are managed at X. The results of this will contribute towards a better understanding of the processes run by different departments across the College.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identity subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>How satisfied are you with the way that the College manages your identity? How effective do you find it to use our various services, such as the library, IT systems, or the College administration? We would very much like to talk to you regarding your experience of X's use of your personal data and information - for example, occasions when someone at the College asks you to prove who you are, or requests personal information from you.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identity user</th>
</tr>
</thead>
<tbody>
<tr>
<td>We would very much like to talk to you about your experience of X's use of personal data and information - for example, occasions when you or your colleagues need to ask someone to prove who they are in the course of your work. If you are not the best person for me to talk to about these matters, I would be grateful if you would forward this message to anyone in your department who might be interested in participating as an interviewee regarding their experience of X's use of their personal data and information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identity provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>We would very much like to talk to you about your experience of identity management at X. In particular we are interested in the [thing we are interested in] system, and in the rules and guidelines (formal and informal, written or otherwise) which you use to manage personal information. If you yourself are not the best person for me to talk to about these matters, I would be grateful if you would suggest one of your colleagues might be able to participate as an interviewee.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identity manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>We would very much like to talk to someone in [unitname] regarding your experience of identity management at X, such as information [unitname] keeps about individuals which is used by them to gain access to physical or electronic resources, (for example the [thing we are interested in] system) and also about rules and guidelines (formal and informal, written or otherwise) used to manage information about individuals. If you yourself are not the best person for me to talk to about these matters, I would be grateful if you would suggest someone in your department who might be able to participate as an interviewee.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Conclusion</th>
</tr>
</thead>
</table>
| If you are able to participate, please respond to this mail, and I'll contact you soon to arrange a date and time we can meet. I'd like to talk with you informally for up to an
Apparently reluctant interviewees will generally be busy rather than unwilling. The KR will need to be flexible about scheduling, even if necessary being willing to have an exceptional meeting outside the time allocated to interviewing in their timetable. However, if they do so, they will need to remember that doing so could easily cause the audit as a whole to slip, either because there are too many exceptions of this form or because time required for analysis is taken up completing outstanding interviews.

5.5.3 Interviewing

**Interview Process**

Each interview should be carried out in a location which makes the interviewee comfortable, but one which is likely to be free from interruption. However, interviews can be carried out without complete privacy, and informal settings have been used in some audits to help put interviewees at their ease.

One of the issues that may worry interviewees is that of anonymity. If interviewees were only willing to provide information that paints the institution in a good light, then much of the purpose of an audit will be unsatisfied. To find out where there are problems, it is necessary to allow the data from the interviews to be anonymised. More anonymity is possible in a consortium situation, where embarrassing discoveries can be discussed divorced from their institutional context. However, it may well be more difficult within an institution: when a comment clearly originates from someone working in MIS, it is going to be easy to pick out the individual who made it. The decision made about report publication (as described above in the preparation stage of the audit) will be an important factor in what interviewees can be offered in terms of anonymity.

A balance needs to be struck between an interview process which is exhausting for both KR and interviewee, and one which does not elicit much useful information. This is the reason why the interview length in the Identity Project was fixed at approximately one hour. It may well be possible for some interviews to overrun; others may take less time. It is also possible to follow up by email or phone where necessary.

It is best to leave the questions open and let the interviewee talk freely, to avoid leading or closing the topics under discussion.

Interviews should be recorded if possible, as this makes the interview process itself easier: the interviewer can concentrate on the discussion rather than needing to make notes. Interview recordings should ideally be archived, in case they were required later, and notes or transcriptions made from them. Interviewees can be given the option of having the recording wiped rather than stored, and of not having the recording made in the first place if they wish (as a part of the anonymity mentioned above). It is also possible that institutional culture is antagonistic to the archiving of this type of recording, in which case they should not be kept once notes have been made. Whether or not interviews are recorded, it is important that the content is documented as soon as possible after the interview, to ensure that relevant detail is not lost.

Expensive recording equipment is not needed for this purpose; many small voice recorders without separate microphones are likely to be of a high enough standard.

**Dealing With Difficult Interviewees**

Even though every effort has been made to make interviewees comfortable, some may still be difficult to discuss IdM with. The major causes of this are likely to be the interviewees' busy timetables, or their feelings that the audit might have negative consequences for their job (particularly if they are conscious that there are IdM shortcomings in their department).

**Busy Interviewees**

The KR needs to make every possible effort to be as efficient and professional as possible. Punctuality, having questions ready, being able to explain the purpose of the audit simple, and knowing enough about the IdM background to talk to the interviewee (both for interviewees who have less technical knowledge than the KR who may need further explanation of some questions, and for those who have more, who will not want to
spend much of the interview time explaining things they think are obvious to the KR) are all necessary requirements for this. Every effort should be made to complete the interviews within the time allotted. All this is a reason for the KR to schedule early interviews with people they already know, so that experience can be gained in a friendly atmosphere.

Where an interviewee continues to be difficult to communicate with, the KR should suggest re-scheduling the discussion to a less busy time, or give the option of an interview by email (which can suit some people, as they don’t need to find the whole time in a single chunk, but which tends to be more difficult for the KR to manage).

**Worried Interviewees**

Interviewees may feel that the outcomes of an audit, if negative, might lead to changes which could include cutting their position. This is partly due to the connotations of the word “audit”, which suggests that it is intended to lead to cost cutting measures. It should be emphasised that the audit is purely an information gathering exercise, which may lead to work being done to amend the business processes but which is unlikely to result in any job cuts in the short term. The KR needs to be polite and pleasant, and should never put pressure on interviewees: the audit is not a piece of political journalism.

Where an interviewee continues to be difficult, it may help to point out senior management support (judgement needs to be used, as this could also be counter-productive). In severe cases, ending the interview and scheduling one with another individual - the line manager of the person who was difficult, for example - might be necessary.

**Interview Templates**

The diversity of IdM across institutions means that a specified set of questions to ask would be inappropriate. It is also the case that interesting information is often elicited through open questions with extended answers that would be missed by a closed question with a short answer. With this in mind, the Toolkit provides a collection of interview templates, designed to catch useful information about business processes, technical issues and unmet requirements. **These templates are not intended to include questions to be asked directly of the interviewee, but are for the benefit of the KR.** In particular, the examples given are intended to suggest the kind of answers that are being sought. It is however quite likely that the KR may consider that the templates are best used, however, as the basis for a number of more rigorous scripts which are used where appropriate (e.g. ensuring that the technical level of the question and interviewee match).

The questions listed in the template given below are generally pretty open in nature, especially the first four, aiming to encourage the interviewee to talk at some length about their IdM role. Some interviewees and some interviewers might well be more comfortable with a more closed style of interview, though this would need to be more closely customised by the institution and for each interviewee, as such questions as “How is a new user added to the central database, and how is the information there used to feed into network account creation?” require the interviewer to know a fair amount about the interviewee's work beforehand. For each of the questions below, a closed alternative is given, to help inspire the creation of a specific template for an interview if this is considered preferable.

The questions to determine unmet requirements are given as a series of supplemental questions accompanying the business processes and technical questions. In introducing the idea of unmet requirements in the interview, we recommend drawing the distinction between requirements agreed on by those running and using the output of the system (Formal requirements), and requirements that the interviewee perceives may be “nice to have” (Perceived requirements).

In some cases the unmet requirements supplemental question is close to one of the supplemental questions to the original question (especially B1), we have included them as we see a distinction in the scope.

**Question Areas for Business Processes**

1. Could you please describe how you ensure that the right people are using the right services?

   [This question is to start a conversation flow. An interviewee is more likely to be open if given such an open question with no pressure from the start. Usually, such an open question gives a lot of information, which may answer some of the questions below as well.]

   Aiming to discover all activities related to those of Core IdM system components, including similar activities
which are not actually carried out as part of those components (whether duplication of these activities or not).

Closed alternative example: Please describe how the information in the Human Resources database is used throughout the process from application to interview to appointment or rejection.

Supplementary questions:

- 1a. How do you ensure that people who are entitled to services have actual access to them?
  
  [Example: What steps does a person have to go through to get the access to which they’re entitled? An example would be that a library user has to have the barcode from their access card entered on the library access system, and they have to have the correct user status entered on the library record associated with that barcode.]

- 1b. How do you ensure that people who are not entitled to services do not abuse your service provision?
  
  [Example: What gateway(s) does a user have to pass through to use the service? How do you stop former users from using the service when they are no longer entitled to? Eg expiry dates on the system.]

- 1c. (Unmet requirements) Are you aware of any people who are in theory entitled to services who cannot access them? [This is similar to 1a, but the thrust of the question is somewhat different.]

- 1d. (Unmet requirements) Are you aware of any people not entitled to use your services, who are, and are difficult or impossible to stop? [This is similar to 1b, but the thrust of the question is somewhat different.]

2. What happens when a user changes status and/or requires a change in their access rights?

Aiming to discover how change control happens in Identity Repository systems.

Closed alternative example: How would the directory information about a user be updated if they move to a new position within the College?

Supplementary questions:

- 2a. What happens if a user role is completely changed, e.g. moving from undergraduate to alumni, or PhD student, having completed the degree, to lecturer?

- 2b. What happens if a user role is extended, e.g. a PhD student also becomes a Research Assistant?

- 2c. Can you explain whether there are differences in handling such cases, if the change requires change in provisioning?

- 2d. (Unmet requirements) Are there any changes of status which when captured by your systems/processes are not automatically propagated, but should be?

3. Do you manage/control more than ONE method of identifying the users of your services? (e.g. more than one log in system, paper-based user records, etc)

Aiming to discover whether an interviewee handles more than one process.

[Example: student ID card, library card, user log in, and so on.]

Closed alternative example: Do you store data about the users of the Finance system in paper files as well as in the database of budget holders itself?

This question aims to uncover whether there is more than one process - it does not attempt to test for duplication of effort or contradictions.

Supplementary question:

- 3a. (Unmet requirements) Are there any systems/processes which have more than one authentication alternative that need to be reduced to a single one?

For the following questions, KRs should decide whether or not to use the term "IdM practices". For some interviewees, the term (with an explanation) might be understood, whereas for others, the KR may need to use simplified terminology.

4. How 'good' are your IdM practices? Have you received any complaints from end users? How
frequent are security breaches?

Closed alternative example: There was an email outage last week. Was that related to any problems with the user data in the system?

Aiming to identify problems with the current process(es) through warning signs such as user complaints or security breaches.

5. Is there any duplication of effort between any of the processes / IdM related functions? Can you give examples?

Aiming to discover any duplication of processes (or parts of processes).

[Example: a paper version of a user record is stored as well as the system entry, but the system entry can be updated without updating the paper copy.]

6. Have you ever encountered a conflict between different IdM practices? Can you give examples? How often does this happen?

Aiming to discover any conflicts between IdM processes (may arise from duplication or multiple processes).

[Example: the user has their privileges revoked in one place but not another.]

Supplementary question:

• 6a. (Unmet requirements) Do your systems/processes need to be amended so that different routes of authentication don't give different levels or types of authorisation?

7. Are there any holes in your IdM practices? E.g. people who are not entitled to services can get round the IdM system? Can you give examples?

Aiming to discover the completeness (or otherwise) of the IdM process.

[Example: people without a valid library card can access the building by giving their word that they are visiting the public museum in the same building.]

8. What controls and indicators do you use to ensure a good oversight of your IdM practices?

Aiming to discover how the process(es) is(are) optimised.

Supplementary questions:

• 8a. Do you record anything?
• 8b. What sort of statistics do you run? How often?
• 8c. Do you hold reviews/audits? How often?
• 8d. (Unmet requirements) Do you need monitoring or control systems/processes that are either unavailable or not currently implemented?

For each major IdM task identified:

9. Can you estimate how long this task takes each time it is required? How many times a year does it need to be carried out? What staff grades are involved?

Aiming to obtain a quantitative measure of the cost in time and money of process(es). For particular interviewees, other measurements may be of interest, such as the number of contractors and visitors present in the institution on an average day. However, note that in practice it has been seen that questions like these "produced much guesswork, mumbling and vagueness from most interviewees".

**Question Areas for Technical Systems**

10. Is there official documentation describing how the system works?

If the answer to this question is "yes", then a lot of the rest of what follows may be unnecessary or run slightly differently. It might be a good idea to ask this before the interview, in order to familiarise yourself with it as much as possible beforehand - especially as you'll want to get hold of this documentation and it might
not be easy to do so during the interview.

**Sample answer:** Yes, and it’s at the URL .... available only through the institution’s intranet. (The KR will need to check the confidentiality status of the documentation if there is any.)

**Supplementary questions:**

- **10a. If not, can you describe how the system works?**
  
  **Sample answer:** A diagram will almost certainly be the best answer here. We’re generally looking for an explanation along the lines of how the various components fit together.

- **10b. Does it link into other systems in the institution? Outside the institution?**
  
  **Sample answer:** Yes, access to past exam papers on the web uses this as a directory to work out who is a student. In turn, this directory collates information from the student databases held by the MIS departments in the several institutions which share courses with us.

  Note: this is deliberately phrased somewhat more widely than IdM (as some of the other systems will not necessarily themselves perform IdM), but we are obviously going to be most interested in answers within the general scope of the project.

- **10c. What are the technical means used to establish the identity of users of the system and the privileges they hold?**
  
  **Sample answer:** The exam papers web server makes an encrypted request using SOAP containing details of the student and the course, which is used to construct SQL queries sent to the databases which hold information on students who have take the course. The system returns a yes/no answer - whether the student is taking the course.

- **10d. Who are the vendors of the different components of the system, or are parts of it developed in house?**
  
  **Sample answer:** This component is a customised version of Soandso’s DoEverything product, and this one is developed in house to cover the functions missing from DoEverything.

  [Note: These questions are grouped because the supplemental questions are intended to ensure that a certain level of detail is apparent in the answer to the main question.]

**10e. (Unmet requirements) If documentation is insufficient, how do first line support or front facing staff know what to do in an atypical situation?**

**11. What maintenance tasks need to be carried out? How time consuming are they, as a rough estimate?**

**Sample answer:** We receive software updates every six months from Soandso which are tested on a trial system before the production system is upgraded. This takes about 1 day to install, and 5 days to test.

  [Note: There may be different answers for different components! This is asking about updates to components, not changes to the nature of the component, for which see question 3.]

**Supplementary question:**

- **11a. (Unmet requirements) Are any required maintenance tasks typically missed either through lack of time or means?**

**12. How long has the system been in use?**

**Sample answer:** Five years in its present form. Before that, we had a less integrated system that needed more manual intervention.

**Supplementary questions:**

- **12a. Do you know of any major changes/updates in that time?**
  
  **Sample answer:** Yes, we changed this component from the Defunctco to the Soandso DoEverything product two years ago when they went out of business.

- **12b. If so, can you describe the update procedure?**
  
  **Sample answer:** We produced a list of requirements (available here but confidential) and put it out to tender. Soandso met more of the requirements than any other bidder. We spent six months writing...
the missing components...

- 12c. (Unmet requirements) Is there any intention of upgrading the system further, or purchasing optional modules for off-the-shelf packages, to enhance functionality?

13. Are users able to update their own information held in the system?
The expected answer here is a yes/no. However there are more substantive supplementary questions:

- 13a. If so, is there user documentation / help pages? (The KR will need to check the confidentiality status of the documentation if there is any.) If not, perhaps it would be a good idea to see a demonstration of how this is done: perhaps there should be documentation!

- 13b. (Unmet requirements) Are there users who might need to update their information but have no route through which to do so?

14. Could you describe any cases of identity abuse which affect this system that you know about?
*Sample answer:* There have been problems with password sharing among students. We know this from analysis of the log files combined with anonymous surveys of users.

- 14a. What steps have been taken to secure this system against identity abuse?
  *Sample answer:* We have contributed to a project to educate users about the dangers of password sharing.

15. What would you change about the system if you had the opportunity?
*Sample answer:* We would like it to be easier to integrate the system with the student databases at the various participant institutions. Currently, we have to write a customised interface for each one, and this is not a sensible use of time.

5.5.4 Organising Interview Material

The organisation of the material generated through the interviews is of vital importance to the successful production of an audit report. Although the KR is probably going to remember the main themes of each interview, it is likely that other matters will be referred to, and it is unproductive to have to search back through all the interview notes for such secondary issues. The Identity Project used a WIKI for the storage of interview data, and instituted a systematic use of tags to indicate subject areas discussed in interviews and documentation. For a single audit, the WIKI model probably involves too much overhead to be useful (unless the institution already runs a WIKI which has a restricted access section that could be used for the purpose), but it would be worthwhile for the KR to keep a record of the topics touched on in each interview, say with a separate index document. The topics to be used need to be determined by the organisation of the report, so that needs to be decided at least in principle before the interviews take place. (Suggestions on ways to do this follow in the section "Phase 4: Identity Management Analysis").

This type of organisation is likely to be of particular importance for the interviews with those who are considered end-users of IdM, where comments made will range across many of the different topics covered by the audit (and quite possibly beyond the scope of the audit as well).

The KR will need to decide how they wish to make a textual version of a recorded interview. A transcript may be useful, but takes time to produce: about four times the length of the interview itself, according to one of the Identity Project KRs. Notes are generally going to be sufficient, and it might well be useful for them to include information about the position in the recording, if later reference to the source material is required. (For example, the indication in the notes that "The process has limitations (25:10)" is useful to find the place where it is discussed if it later turns out that the KR wants to know what the limitations are.)

5.5.5 Checklist

By the completion of this phase, the following should be ready:

- A short list of contacts for interview
- A collection of interview recordings and transcripts/notes
5.6 Phase 4: Identity Management Analysis

The main task in this phase is to create a report based on the interviews and documentation, which can then be signed off by the body which has oversight of the audit. In this section, we describe one possible structure for such a report, which is intended to be advisory rather than prescriptive. Clearly, specific approaches to an audit (e.g. a driving need to investigate one particular issue) will lead to different structures for a report, and some parts of the report structure given here may not be relevant to smaller or specialised institutions, or where a cut down version of the audit was undertaken. However, the topic based approach is still likely to be useful, if only to indicate what needs to be covered. (It may be useful to indicate that a section of the suggested report is not relevant because no Identity Management fitting into the section’s topic was found at the institution, especially for topics such as X.509 certificate use.)

When planning a local structure for the report, it should also be remembered that setting the topics for the report before carrying out the interviews is likely to prove problematic, as it is then harder to fit the interview material into the report structure; when an institution is carrying out its own audit without reference to external requirements, it should be possible to tailor the structure of the report much more closely to fit the IdM discovered by the interviews.

5.6.1 Report template

A suggested template for the final report would be to include the following sections. For each section of the main body of the report, relevant links are given to the IdM governance and IdM systems sections of this Toolkit.

1. Executive summary.
2. Methodology. This section outlines the process of information gathering for the case study, as prepared for publication. It should include:
   - a commentary on the audit process itself, particularly any features which stand out about the process as applied to the institution which carried out the audit (in particular, any major divergence from the process given here should be described).
   - information about what was left out (including scoping decisions, and some idea of which contacts were not interviewed)
   - a list of anonymised references used to indicate the different interviewees and respondents with some indication of the functions carried out by them (enough to give an idea of how authoritative their comments are without compromising their anonymity). This list will then be referred to throughout the audit report and should give a substantive background to the report’s discussion of IdM. (The KR may decide that this information fits better in an appendix.)
3. General Description of the Institution. This section includes an overview of the institution’s record and management systems (a broad overview of its IdM regime), and a description which places the institution within the context of UK higher education generally.
4. Managing Identity Information. Including:
   - 4a) Identity repositories, attribute stores and usage. This section examines how user attributes are stored, used and disclosed. See also Identity Repository and Lifecycle Management.
   - 4b) Handling of identity for individuals not classed as staff/student (academic and library visitors, contractors, etc). This section analyses the variation that exists between external users, their processing, levels of access and particular problems faced in their management. See also Contractors, partners, other third parties.
   - 4c) Handling of prior ID discovery for new users (e.g. postgraduate students who were prior undergraduate applicants) and of potentially competing ID generation by different parts of the institution (such as the Library and MIS). This section examines the extent to which any previous ID is used by the institution, the extent to which it is done comprehensively and accurately, the mechanisms used to do this and the amount of information released to the user.
5. **Integration.** Including:

- **5a) Identity security and privacy issues.** The various mechanisms used to transport attribute information, how decisions are made about what attribute to release to whom and the attitude of service users regarding the transfer of such information.

- **5b) Single institution and cross institution Virtual Organisations and tools.** The different communities and cross-institutional work that operate within the institution and how they are supported.

- **5c) Collaborative learning.** The use of IdM in collaborative learning schemes within the institution.

- **5d) Integrating UK HE identity management with other communities (including NHS, overseas integration requirements), including problems requiring further work, standardisation issues, etc.** The other communities with which the institution works otherwise overlooked in this report their impact on identity management.

- **5e) Personal Identity Management and managing identity across institutional boundaries (cross-affiliation): use cases in UK HE, including role management requirements; use cases between UK HE and other sectors.** This section considers the scope for personal identity management by institution members and the issue of multiple identities. This includes use of OpenID, facebook identities, personal email addresses, etc.

6. **Security and Access Control.**

- **6a) Credential management.** The use, issue and expiry of user credentials along with their safeguards against their misuse and procedures for revocation. See also Identity Repository and Lifecycle Management.

- **6b) Certificate management.** The extent to which X.509 certificate management in the institution may operate (as personal authentication tokens) (where practised).

- **6c) Requirements for use of credentials including resource access, technological requirements (e.g. single sign on, stability and scalability), accounting and statistics, etc.** How the requirements and procedures for the use of IDM technology are determined. Other sections of this Toolkit will be useful for reference here, as they deal with idealised requirements for such systems: IdM requirements and solutions.

7. **Compliance and Governance.** Including:

- **7a) Policy Audit.** Describing which relevant policies exist and how to access them if not public.

- **7b) Audit Regime.** Describing any measures are taken to ensure policy is followed, detect and prevent mis-use.

8. **Conclusions and Recommendations.** This section examines the main themes drawn from the report and suggests some considerations for future work. It should answer the following questions:

- What is good about current practice?

- Where are there gaps in current IdM provision? (This may be better kept in a separate gap analysis report.)

- What can be done about them?

### 5.6.2 Useful information to include

Appendices to this structure can include breakdowns of the time spent on the audit by the KR; glossaries; and links to IdM policy documents published by the institution discovered as part of the audit. The glossary is often necessary not just because some IdM terms may not be transparent, but also because institutions often have names for particular systems (such as Imperial College’s Son of Validate) which are likely to be meaningless to many readers, including some in the institution itself. A list of known restrictions and access conditions to IdM practices (particularly credential management) which arise from sources such as resource licenses or Service Provider access conditions to help ensure compliance would be likely to be a useful resource for future IdM management planning, and would form a useful appendix.

72 of 123
Relating this report structure to the lists of questions used in interviews (see the investigation section) is not entirely straightforward, because the questions are intended to be adaptable for many different interviewees, and the divisions in the report structure relate more to ways of classifying the interviewees themselves. So we give a table here relating the core functions listed in the discovery section to the sections of the report. An “X” in the box indicates that interviewees involved in the given core function are likely to produce answers of relevance to the completion of the report section. These are merely suggestions, however, and it may well be that there will be other relevant interviews for each section of the report (e.g. from minor systems related to a core function, such as a human resources website which uses attribute information to give members of the institution easy access to make job applications), and ones listed which turn out not to be relevant in particular cases.

<table>
<thead>
<tr>
<th>Core function</th>
<th>Report Section</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
</tr>
<tr>
<td>student record system</td>
<td>X</td>
</tr>
<tr>
<td>human resources / personnel</td>
<td>X</td>
</tr>
<tr>
<td>email/network account provisioning</td>
<td>X</td>
</tr>
<tr>
<td>management of physical access to buildings</td>
<td>-</td>
</tr>
<tr>
<td>management of library resource access</td>
<td>-</td>
</tr>
<tr>
<td>VLE and/or portal management</td>
<td>-</td>
</tr>
<tr>
<td>alumni records / development office</td>
<td>-</td>
</tr>
<tr>
<td>finance/payroll</td>
<td>-</td>
</tr>
</tbody>
</table>

Organisation of the interview material is key to the production of a successful report. The reasoning behind this and suggestions for methodology are described in the section Organising Interview Material. With the use of tagging, or an equivalent, it should now be possible to sort out the material from interviews (and documentation) which is relevant to each of the sections for the report.

### 5.6.3 Checklist

By the completion of this phase, the following should be ready:

- The final report for the audit, including conclusions and recommendations, as accepted and published (in the way decided at the start of the audit) by the advisory group

### 5.7 Acknowledgements

The material in this section is adapted from the outputs of the Identity Project. Principal authors include Simon McLeish (LSE), Margaret Flett (University College London), Guy Burton (LSE), Greg Pytel (LSE), Rhys Smith (Cardiff University), Ken Brown (Birkbeck College), Ian Casselton (Royal Holloway, University of London) and John Harmer (School of Oriental and African Studies).
6 Gap Analysis

6.1 Introduction

Executive Summary

A gap analysis consists of three parts: an understanding of the current state of affairs, an understanding of the desired state of affairs, and the development of a method to get from the first to the second. For IdM at an FHE institution, all three will depend to a significant extent on local conditions, which cannot be developed here. In this section, we look at means to establish the current and desired states of affairs for IdM, give a list of common gaps (derived from the work carried out by the Identity Project), and make some suggestions as to how a strategy can be developed.

Section contents:

- 6.1 Introduction
- 6.2 Establishing Actual Performance: Outlines methods to use to determine current performance of IdM.
- 6.3 Establishing Potential Performance: Describes the requirements which should help determine potential performance.
- 6.4 Common Gaps: The common gaps in IdM practice as determined by the Identity Project through a sector-wide survey and in depth audits.
- 6.5 Producing a Gap Analysis Report: How to turn this information into a gap analysis report.

The purpose of the audit defined in the previous section is to establish exactly what IdM functions are carried out in an institution. Once this process is complete, it is necessary for those responsible for IdM in the institution to establish the gaps between actual and potential performance.

In this section, “gap analysis” is taken to have the meaning it carries in business process analysis, viz. a “business resource assessment tool enabling a company to compare its actual performance with its potential performance”\(^2\). Naturally, how an institution analyses this difference in terms of IdM will depend on both the actual performance (as determined, for example, by an audit) and the desired potential performance (e.g. adherence to ISO 27002\(^2\)).

6.2 Establishing Actual Performance

6.2.1 Using the Audit Report

If an audit has been carried out, it is likely to have provided a good picture of the details of many identity management practices in the institution, and it will have made recommendations to an appropriate body within the institution (such as an IT Managers committee). It has certain limitations and institutions may want to consider combining it with other information to inform the gap analysis.

6.2.2 Outcomes from Other Sources

Other methods can also be used to discover information about the institution’s IdM performance. Examples include:

- **Password experiment**\(^2\) This is a method to measure the state of knowledge about security and privacy among end users.


\(^{22}\) [http://www.27000.org/](http://www.27000.org/)

• **Use of existing surveys** Many institutions carry out periodic (frequently annual) surveys of user satisfaction with IT Services departments. Questions relating to IdM practices can be inserted into such a survey. Questions that would be appropriate will depend on the general format of the survey (e.g. whether short questions where users choose one from a range of options are preferred), but it might be possible to choose some from the following:
  
  - How satisfied are you that the institution is protecting your privacy/security online?
  - Have you suffered from problems accessing resources (physical or electronic) which you should have been entitled to access during the past year? (If so give details.)
  - Have you changed your password in the past year?
  - How satisfied are you with the institution's procedures for managing your identity?

• **Analysis of help desk enquiries** where these relate to IdM. Where help desk software is used which allows categorisation of the type of a query, this becomes a comparatively simple task - and provides useful measures of a reasonable degree of accuracy which can be gathered over a lengthy period of time - providing that IdM is one of (or a subset of) the permitted types.

• **Keeping records of a variety of IdM related metrics** over a period of time. This would be particularly useful for measuring the effectiveness that work on IdM has in improving the situation. Naturally, the metrics to be used (and how they're measured) would depend on the nature of the gap involved, and the figures will not necessarily indicate the presence or absence of a gap (as there are no benchmarks to measure them against). Some ideas of metrics which could be used for this purpose include:
  
  - the number of inactive user accounts in a system (where “inactive” is given a precise meaning such as “not accessed in the preceding six months”)
  - the time to create a new user (again, what “create” means would need to be precisely defined, as this could mean: from enrolment to creation of a student record, or to the creation of a network user account, or to the user being able to receive email sent to an institutional address)
  - the number of times an IdM process requires intervention per month (particularly useful for supposedly automated processes)

There are many resources on the Internet which make suggestions on how to write a business case for identity management (mainly aimed at businesses rather than the public sector). Some recommended examples include:

- The Gartner report "Justify Identity Management Investment with Metrics" by Roberta J. Witty, Kris Brittain and Ant Allan, 2004 (Gartner Research ID number TG-22-1617).

Using these tools would provide more statistically accurate measures of how users view the institution's IdM practices and gives more emphasis to the opinions of end users than an audit can provide. It is more difficult to find a method by which the other problem from which an audit suffers, the tendency of interviewees to concentrate on what should be done rather than what is done in practice, can be compensated for. Observation of identity managers at work, for example, is likely to be intrusive, expensive and of relatively little value; use of "mystery shoppers" is likely to be expensive and a potential security hole in itself.

For both these options and the audit itself, repetition of the measurement activities periodically should give a better picture of the way that things are changing than carrying any of them out once only. When repeating an activity, it is important to do so as closely as possible to the original version, because changes will make comparison of the two iterations less valid. Some changes may however be desirable; in particular, there may be new developments in IdM or local infrastructure which need to be taken into account.
6.3 Establishing Potential Performance

In the UK FHEI context, the minimal potential performance should be based on:

- **legal and regulatory requirements.** Some information about these is given in the introductory section of this Toolkit, but the institution's Data Protection Officer will be able to describe the details of how they apply and should know how IdM systems relate to them.

- **contractual requirements necessary to carry out the normal activities of a UK FHEI** (e.g. adherence to stipulations in electronic resource licenses purchased by the library - though these are not always written with IdM security in mind and it may be the case that it would be preferable to renegotiate some than comply to the letter)

- **the requirements (and recommendations) for UK Federation membership**, listed at [http://www.ukfederation.org.uk/content/Documents/FedDocs](http://www.ukfederation.org.uk/content/Documents/FedDocs) - in particular the rules of membership and the recommendations for use of personal data. It should also be remembered that decisions made by an institution as an Identity Provider will affect the way that institutional members are described to Service Providers, and thus the design of any IdM work needs to ensure that it will not affect the access of members to external resources. In the Federated Access Model, a Service Provider is dependent on the quality of the IdM processes of the Identity Providers used to access its resources.

The systems, components and functions section of the Toolkit, describing the components of an ideal system, is likely to help identify technical gaps. This description will need to be analysed to see which components give appropriate requirements for the IdM of the specific institution. Generic requirements are gathered together in Section 4, Defining Institutional Requirements, and these can also be used as a basis for establishing potential performance.

Many institutions will already have ideas about where gaps exist, and these will often be directly pointed out by interviewees in an IdM audit. However, it is difficult to produce a gap analysis without a clear idea of the potential performance requirements, and for this purposes an institutional IdM strategy is an invaluable aid. Some suggestions which may aid the formulation of an IdM strategy can be found in the Toolkit section on governance. (Of course, the lack of an overall strategy may be one of the gaps that needs to be addressed.)

6.4 Common Gaps

The JISC funded Identity Project carried out a number of audits following the model described in this Toolkit in UK FHEIs during 2007 in conjunction with a survey sent to all UK FHEIs. It is clear from these audits and the survey that institutions are likely to find gaps, and that some are common to many institutions. The project's report Common Problems/Solutions, Best Practice, Future Developments (no longer available) collected these issues together; a summary is given here.

One topic which has achieved prominence since the conclusion of the Identity Project is the relationship between institutional IdM and external systems utilised by many of the institution's users but not controlled by the institution, such as Facebook, OpenID and other social media sites and technologies, especially as it starts to become possible to embed institutional services in them (such as Facebook applications listing library books the user has out) or use them for access to other systems which may seem more official (such as Google Docs stores of documents produced by academics available to students, or twitter hash tags for discussion of courses).

Clearly, there may be other gaps which are specific to a particular institution, and these should also be considered. Tools such as the audit should uncover these gaps almost as readily as those which occur in many FHEIs. It is also likely that the different local situations make it sensible to subdivide some of these gaps, or that there will be specific local issues which need to be listed.

Some suggestions are made for work which could be done to close each of these gaps, and a list of likely stakeholders who will need to be consulted. The suggested work is not intended to be prescriptive, but is intended to give some ideas which can be elaborated on as wished in a particular institutional setting.

---


6.4.1 Gaps Linked to IdM Governance

Lack of Commonality of Definition of "Identity Management"

Many practitioners of Identity Management, in the wide sense used in this Toolkit, may well restrict the term to a smaller subset of processes, such as account provisioning or physical access. There is also a tendency to think of IdM as part of the IT infrastructure, rather than as a collection of business processes. Managers of processes with an identity component often act as though IdM is restricted to the type of identity management which is instantiated in that component (for example, those who control electronic door locking systems tend to think first and foremost of access to physical access when IdM is mentioned). This can lead to misunderstandings in the process of management and administration of IdM related projects, as the different people involved in planning, management and execution of the project have differing ideas as to the scope of the project.

Suggested work: Establish an agreed definition in an institutional IdM strategy document. Produce a briefing for those who have a need to understand IdM. This would also serve to act as a pointer to institutional IdM policy documents relating to IdM.

Stakeholders: Departments involved in central IdM, particularly HR, IT Services, Registry (this group is referred to as "central IdM practitioners" in the remainder of this section, for brevity). Managers who might otherwise localise IdM activities for the people in their group (an important target for the briefing).

6.4.2 Gaps Linked to IdM Policy

Formal Procedures

Most, if not all, institutions will have some kind of existing formal procedures covering IdM. However:

- these may not cover all the IdM related areas
- these are not translated into actual processes or technical specifications
- these are not enforced throughout the organisation
- ownership of processes, data and documentation is not always clear

The existence of such procedures is a requirement of ISO 27001.

Where IdM procedures are informal and undocumented, they are also likely to be:

- poorly understood (both by practitioners and management, and certainly by other users of any personal information stored as a result of the process)
- without overall control
- more likely to contain security holes due to a lack of oversight
- vulnerable to turnover in key staff
- less easily integrated with other processes in the institution, whether IdM related or not.

Documentation is likely to be stronger in areas considered particularly sensitive (such as Finance) than in areas which are less fully developed (such as IT Services, which has a comparatively short history) or less clearly needing attention and oversight (e.g. access to resources within an academic department).

Suggested work: Education of IdM practitioners in the importance of documented procedures and policies. Establishment of a group to manage production, adoption, publication and publicising of procedures and policies. Draft and adopt policies to fill known gaps (e.g. based on the lists in the Governance and Policy Toolkit section).

Stakeholders: Senior management. Central IdM practitioners.
6.4.3 Gaps Linked to IdM Strategy

**Heterogeneity - Independent, Disparate Systems**

Institutions consist of a number of faculties, departments, centres, research groups etc., which may run IdM solutions which meet specific local needs and which are to some degree independent of central systems. This results in a number of systems, which are not supported by the central administration team responsible for IdM. It should be noted however that there are also situations where heterogeneity is beneficial for security reasons. This means that some critical systems (e.g. in finance departments) and systems storing sensitive information (e.g. registries) are usually kept outside of the central IdM administration, and should probably remain so.

Where multiple identity records for the same individual are created intentionally (i.e. with the backing of proper procedures), they need to be properly curated: some record needs to be kept to indicate that two records in different systems refer to a single person; changes in status and expiry needs to be handled in such a way that changes are made to every record at the same time rather than just to one or another. What is more important is that stringent efforts should be made to avoid the unintentional creation of multiple records.

The practical solution that reconciles the heterogeneous management environment (including IdM) with the need of central administration involves:

- good coordination between central system administrators and local systems administrators;
- introduction of a single credentials environment, based on the central system, prospectively leading to the introduction of single sign-on (except for some systems that for security reasons should remain outside of such an environment).

**Suggested work:** Purchase/development of a central IdM solution. Establishment of a committee to oversee IdM. Integration of existing systems into a single sign on regime. Establishment of a directory to be used by applications which consume user attributes, otherwise known as an Enterprise Directory. Documentation of ownership, purpose and use of user attributes.

**Stakeholders:** Central IdM practitioners. Developers and technical managers of applications which use attributes (e.g. VLEs).

**Common Standards and Central IdM Administration**

Different processes and standards (e.g. for person metadata) are implemented by different sections and departments across the institution, usually for historical reasons of decentralisation and independence. This is particularly likely to be a problem across sections of an institution which were separate prior to a merger. Common examples include databases which have a single attribute listing a person's name, where others have separate attributes for surname, given name and/or initials. This leads to:

- inadequate deprovisioning practices (including non revocation of physical access, a serious security issue)
- multiple identities (which was "very common" in some audited institutions)
- non-uniform access across departmental systems within a single institution
- non-unique or inconsistent ID generation (potentially leading to ID ambiguities)
- difficulties in linking data about a single individual across multiple systems and databases

**Suggested work:** Integration of existing systems and standardisation of information held, produced and used by them. Purchase/development of a central IdM solution. Integration of existing systems into a single sign on regime. Establishment of a directory to be used by applications which consume user attributes, otherwise known as an Enterprise Directory. Documentation of standards used in IdM systems. Production, adoption and implementation of IdM policies.

**Stakeholders:** Managers, technical staff and users of systems which are use IdM across an institution. Central IdM practitioners.
6.4.4 Gaps Linked to IdM Technicalities

**Limited Deprovisioning**

Account de-provisioning is likely to be less consistently managed than account provisioning, simply because it is intrinsically a less tidy process, occurring for a wide variety of reasons. But this can lead to problems.

In general, a standard user is likely to be handled quite well. That is, a student who starts a course, and continues being a student until the end of their course; or a member of staff who works through to the end of their contract. Problems are more likely with both students and employees who do not follow the standard path, such as a student who is given an extension to complete a project, or a research student who also becomes a research assistant, or a member of staff assigned duties that are beyond his standard scope of work, which require additional access to resources. In these sorts of cases:

- adding extra rights or an initial extension to an automatic cutoff date is usually straightforward
- removing the extra rights when no longer required, or in some cases, ensuring that the account is terminated according to policies, is not.

Essentially, this is likely to be because the institution's central IdM system is not kept informed of the situation, so that no one with the authority to make manual changes to the user's rights knows that it is time to do so.

Non-standard users are likely to be problematic in every case. These users have a less usual, and often less well defined, relationship with the institution. Typical cases include:

- departed staff (emeritus professors and retired staff generally) and students (alumni); some departments in Identity Project partners are looking at offering professional development courses to alumni, blurring the boundary between current and former students
- honorary academics
- prospective students
- external examiners and members of governing bodies
- conference attendees
- short course and summer school attendees
- consultants contractors, temps, and employees of third party suppliers (e.g. building maintenance staff, catering staff, and cleaners)
- students’ union staff and sabbatical officers
- staff for research centres
- external members of facilities connected with the institution (e.g. sports centre members), especially the library (see below), and members of organisations involved in community projects associated with the institution
- visitors who require access to buildings beyond that permitted to normal members of the public (e.g. open day visitors, exhibition visitors, graduation ceremony guests, guests at functions hosted by the institution or by hirers of institution facilities, the emergency services)

Where a UK institution has links with the NHS, the list of anomalous user types can become far larger.

Note that some users who should be treated as different cases may be placed in the same category by existing processes. For example, there are increasing numbers of UK FHE institutions who are currently providing or planning to provide credentials to students who reside overseas. At the same time, there are electronic resources which have access restrictions which only allow use from the UK, and it is important that the attributes of these users reflect their out of UK status and that the institution’s Identity Providers therefore do not assert that they have rights which they should not have.

**Suggested work:** Drafting, adoption and implementation of policies on management of anomalous users. Briefing sessions and training for those who manage such users. Integration of systems used to manage
such users with central IdM solutions.

**Stakeholders:** Those who run systems which manage anomalous users (the list of typical cases above will suggest who these should be in an institution). Central IdM practitioners. Users who fall into these categories.

**Identity Management Data Quality**

Frequent instances are likely to be found where data is incorrect, inaccurate, or not fit for purpose. Errors are often connected to manual input of data, and lack of fitness to re-purposing of data from one application (where it is well understood) to another (where understanding is lacking). Full comprehension of data which is needed before re-purposing includes such things as an understanding of how the information changes over the cycle of the academic year, how the information is updated and how much timelag this update might have, what every state of information means, and what permission a system has to pass on this information to other systems.

To give an example, a student records system may have been developed to meet a historical requirement from the Registry office that the data from student enrolments to course modules be correct by the production of an official timetable in November. This means that another application, such as a VLE, cannot use the data from this system given that it has a requirement for the data to be accurate on the first day of teaching in October. Where documentation is insufficient, and does not record the accuracy standard of the data in the student record system, it would be likely that the incorrect data is used by the VLE without anyone realising the potential for problems.

**Suggested solutions:** Drafting, adoption and implementation of policies governing data quality, ownership and re-use. Implementation of systems to track inaccuracies (e.g. periodic checks that information about a random individual in different databases matches). Elimination of manual re-keying of data where possible. Integration of systems which re-use data (so that a central data source is used rather than a local database). Implementation of mechanisms for reporting of erroneous data (by users, IT helpdesk personnel, etc.).

**Stakeholders:** Users listed in databases which may hold erroneous information. Managers of databases which contain user attributes. Technical staff managing systems which need to use attribute data. Central IdM practitioners.

**Use of Non-unique User Credentials (simultaneously per individual)**

Many institutions allow individuals to be assigned more than one set of credentials at the same time. A typical example is when a student is also employed by the institution - a second set of credentials is an apparently simple way to make it possible for the new rights they have gained to be exercised.

This process causes problems because different records about each individual concerned may not all be linked to the same credentials, which can make it hard to know that they do indeed refer to the same person. This difficulty can become a serious problem when, for example, there may be legal requirements to discover all the related records, such as when responding to Data Protection Act requests. It is also possible that records may be erroneously linked if naive methods of discovery are used (e.g. checking the equality of small numbers of attributes, such as given name/surname), so that information about two distinct individuals is assumed to be multiple records both connected to one or the other of them.

Sometimes such a regime is a deliberate result of policy, and if so this policy has to be well documented. This documentation should cover:

- the circumstances under which multiple identities are to be created
- watertight methods to correctly link the multiple records belonging to one individual (e.g. a requirement to maintain a central record of multiple identities as and when they are created)

**Suggested solutions:** Drafting, adoption and implementation of policies regarding the creation and management of multiple identities, including guidelines for specification of software purchases to ensure that delivered systems do not require locally held credentials unless this is a requirement stipulated in the policy. Integration of systems into a single sign on regime. Purchase/development of a single IdM solution.

**Stakeholders:** Central IdM practitioners. Managers of systems which require locally held credentials. Individuals managing the purchase of software for the institution.
**Re-use of Identifiers**

When an individual leaves an institution, identifiers (such as email addresses) and credentials assigned to that person may be re-used after a time. This clearly carries risk (such as unintended access for the new user to resources they should not be permitted to access, or receipt of information sent as emails to the former user or to lists to which they were subscribed). Clear policies need to define when such re-use is permitted, and this should take into account recommendations made by bodies such as the UK Access Federation. The Federation rules of membership\(^{26}\) require that an institution which wishes to assert user accountability, then release of unique, persistent user attributes (which may in some cases be derived from usernames etc.) should not occur within 24 months of the last possible use of them by the previous user.

**Suggested solutions:** Drafting, adoption and implementation of policies regarding the re-use of identifiers. Fixes to procedures and associated software for the creation of credentials for new users.

**Stakeholders:** Central IdM practitioners.

### 6.5 Producing a Gap Analysis Report

For each identified gap in performance, the report should include as much as possible of the following information:

1. Description of the current performance (Baseline)
2. Description of change(s) suggested: Changes should have a measurable effect
3. Description of the desired performance (Target)
4. Reason for change (Rationale)
5. Degree of change (i.e. estimates for how difficult will it be to achieve the change, and how beneficial will it be to do so, and whether the gap will be completely filled - which may not be possible in some cases)
6. How to measure that the change is successful

This listing is effectively a template for the gap analysis, and is based on the Goal Gap Analysis found at the Office of Research and Institutional Effectiveness, Butler Community College (no longer available). Ideally, the change should be as objectively measurable as possible, though defining a usable measure may be hard to do and may require work beyond that already carried out. For example, attempting to count the number of entries in a directory which relate to users who have no current connection with the institution is likely to require analysis across several databases, even if there are attributes in the directory which contain expiry dates (since if the expiry date is passed, the record should no longer be accessible; if the record is incorrectly active, the date is almost certain to be incorrect). Counting relevant help desk queries is one method of providing a measure of the severity of the problem.

It is also useful to provide a summary analysis of the gaps for visualisation, and one method of doing so is to give scores for each gap for:

- Fitness: how good is the current practice
- Target: what can reasonably be achieved (measured against perfect performance)

Each of these will differ widely between institutions (and of course the scores given will be arbitrary estimates from the authors of the gap report), but should provide a useful way to present the gap information to senior management. We give a simple sample spreadsheet (Excel format)\(^{27}\) and graphical representation for common gaps.

---


A gap analysis report should also include overall prioritisation of the work to be done; ideas on which gaps could be tackled together; and ideas for including gap filling in other initiatives or work which needs to be done as a matter of course (e.g. with planned upgrades to an existing IT system).
7 An Institutional Roadmap for Identity Management

7.1 Introduction

Executive Summary
This section deals with the production of an overall roadmap or programme plan for the actions an institution needs to take in order to improve identity management. It discusses the prioritising of major deliverables and milestones identified by an audit and gap analysis by factors of achievability, cost and institutional impact.

Section contents

• 7.1 Introduction
• 7.2 What is an IdM roadmap?: Defines a roadmap for IdM
• 7.3 Why is a roadmap useful?: Explains why it makes sense to have one
• 7.4 Target System Types: Explains the different systems a roadmap can target for improvement
• 7.5 Prioritising Targets: How to work out the plan for improvements
• 7.6 Writing an IdM Roadmap: Suggestions for the contents of an IdM Roadmap
• 7.7 Conclusions

Preceding sections of the Toolkit have discussed performing a gap analysis of current IdM practice as compared to desired IdM practice; and using that to inform a plan of work – essentially what work will need to be done to bring an academic institution to the point it would like to be at with regard to IdM. Given this plan of work, the next step is in producing a roadmap for this work. This section gives advice and guidance on how this roadmap can be constructed.

7.2 What is an IdM roadmap?

A roadmap is essentially a document that describes firstly how the future state of IdM should function, and secondly describes a prioritised plan of work that will get IdM to that state. This can be used to split up an IdM implementation strategy into various phases. It should use as input an assessment of the current state of IdM as would be uncovered during an IdM audit and a gap analysis produced from this assessment, along with a description of the required changes needed to fill the identified gaps.

An IdM roadmap should include an implementation timeline with major milestones and key deliverables identified. Other things that need including in a roadmap are an identification of risks and mitigations against those risks and methods for monitoring and measuring progress against the roadmap.

7.3 Why is a roadmap useful?

In many cases, the amount of work necessary to implement and embed a central IdM system within an academic institution is likely to be large and complex. A “big bang” approach to this process - whereby all components are installed and configured in essentially one go - will in almost all cases not be appropriate, as the sheer amount of work and integration necessary will be overwhelming to implementers and users.

Thus, the more sensible approach is a measured, phased approach to implementation with an appropriate pace of change. Constructing a roadmap to prioritise the overall plan of work into such a measured, phased approach will maximise the likelihood of success of an IdM project. This road will identify an order of work that will gradually encompass all of the systems that are ultimately required to be integrated within the overall solution.
7.3.1 Appropriate Pace of change

The experience of those who have already gone through the process of implementing and integrating IdM systems consistently shows that new systems should be connected gradually to an IdM solution.

One of the main reasons for this is that any legacy system - where “legacy” here means any application with any existing data in it - will have its own quirks and intricacies in operation and data that it cannot be hoped to understand in full without the aid of time. Even a full understanding of data within a system at a particular point in time is often not enough - it can take at least one academic cycle (i.e. one year) to understand how that data changes over time. For example, data that is updated in a timely manner during academic term time may be much slower to be updated over the summer break; data that is generally kept up to date throughout the year may suffer timeliness issues at the start of the academic year due to sheer volume of change at this busy time of year; and other such issues causing data quality and timeliness to vary over time.

Ensuring that the pace of change is appropriate to an academic institution, and not needlessly rushing the process, will mean that time can be taken to really understand each component in an IdM system; this knowledge will increase the chances that the IdM implementation will be deemed a success.

7.4 Target System Types

IT systems connected within an IdM implementation can be split conceptually into two main types, Data Authorities and Data Consumers.

Data Authorities are mainly sources of identity data. Within an academic institution, these will usually include the Student Records System (SRS) – the data authority for student identity information – and the HR system – the data authority for staff identity information. Further sources of identity data may include things such as Alumni systems, NHS systems, etc. Also, there will often be systems for manually managing identity data of non-standard users who do not exist within any of the "standard" data authorities.

Data Consumers, on the other hand, are mainly users of identity data. Within an academic institution, these will include things such as network account provisioning/de-provisioning mechanisms, email account management systems, VLEs, institutional identity card systems, physical access systems, etc.

Note that many systems may technically be both a source of, and consumer of, identity information. For example, a SRS may be the authoritative data source for student identity information such as name and address. This information may be consumed by the email account management systems to give that student an email address based on their name, and the email address fed back into the SRS. Thus the email account management system is both a consumer of identity information – the student's name – and an authoritative source of identity information – their email address.

7.5 Prioritising Targets

There are many different systems within an academic institution that an IdM solution could potentially be connected to. The integration of all of these is an end-goal of a long-term IdM strategy. Unless there are only a very small amount of systems, or staff within the academic institution have a great deal of experience with IdM, then a good method is to split this long-term strategy up into separate phases. How gradually this is achieved is a decision that needs to be taken by the institution. Slower is more likely to enable a successful IdM system, but means that benefits will likely take longer to materialise.

7.5.1 Identifying initial targets

The aim of a first phase of IdM implementation would be to establish the core IdM system and identity vault, connected to at least one data authority and one data consumer. This will allow identity data to be provisioned to the identity vault, and this information to be made productive use of by an identity data consuming system.

Getting this first phase implemented in a manner that is deemed successful by all involved is vital for the success of further phases of implementation. Any good experiences will help to achieve future stakeholder buy-in, while bad experiences may sour opinion on the IdM system and make further phases politically more difficult to achieve.

Which particular systems should be targeted can only be assessed within an academic institution however, the following general points can help identify which systems are most appropriate.
**Easiest to Accomplish**

Different systems may be more or less difficult to integrate with an IdM system. Choosing systems which are "easier" to integrate in general will increase the likelihood of successful integration, and thus success of the initial phase as a whole.

To some extent, understanding which will be "easiest" to integrate is a very difficult question that can only be answered by people with existing experience. The two separate points of “Co-operation of Vendor” and “Standards”, as discussed below, may be an influencing factor on this ease of integration. Community support from other academic institutions on the relative ease or difficulties of integrating specific applications may help in this assessment.

**Cost**

Different systems may nominally cost more or less to integrate with an IdM system. While the cost is obviously related to the “easiest to accomplish” point, there is a subtle difference and therefore this factor should also be examined. Remember to take into account internal staff time, external consultancy time, hardware, software, and all other costs associated with integrating a particular system.

Systems should be chosen that fit within the budget of the first phase of IdM implementation.

**Co-operation of Vendor**

Systems purchased from an external vendor that the academic institution does not have control over (i.e. no access to source code, etc) will offer a particular challenge in integrating with an IdM system - it is likely that the vendor may themselves have to make changes to the system to support such integration. Choosing systems whose vendor is more amenable to this idea will increase the likelihood of success of successful integration, for obvious reasons.

**Standards**

Certain systems may be heavily based on open standards, while others may make use of much more closed, proprietary standards (or no published standards at all). Choosing systems which make greater use of open standards will increase the likelihood of success of successful integration, as the amount of effort involved in integrating these systems is likely to prove smaller than those systems which do not.

**Biggest Positive Impact**

Some systems may have more of a positive impact than others when successfully integrated with an IdM system. Choosing systems which have the higher degree of positive impact will increase the success and reputation of the initial phase.

For example, the major source of identity information within an academic institution is usually its Student Records System. Integration of this, rather than the HR system, in the initial phase, may produce more tangible benefits, thus being a “bigger win” for the phase.

**Smallest Negative Impact**

Existing systems will likely have many years of legacy procedures, policy, and data connected to them. Choosing systems which will cause the least amount of change to the working lives of members of an academic institution will decrease the likelihood of causing major disruption and discontent to these members, thus increasing the likelihood of the initial phase being deemed a success.

There is obviously a fine line to be trod between changing procedures and policy for the good – making them more efficient and correct – and taking care not to change things too fast. The correct pace of change can only be assessed from within an organisation.

**Stakeholder buy-in**

Some systems may be run by groups with an understanding of the positive benefits of the integration of their systems within an IdM solution, while some may be run by groups who are very cautious of changing
fundamental aspects of their systems for benefits they do not understand or believe in. Choosing systems which have "buy-in" from the groups responsible for them will increase the likelihood of success of successful integration, as these groups will likely be more willing to work closely with those responsible for implementation and will be less resistant to change.

7.5.2 Secondary targets

If the first phase of implementation was deemed successful, the reputation of Identity Management and the IdM systems put in place should now be well established. A good central IdM system and associated identity vault should now be in place, connected to at least one data authority and one data consuming system.

Given this good reputation, the second phase of implementation, where secondary targets are identified and integrated with the IdM system, can afford to be a bit more ambitious than the first phase. Systems deemed as harder to integrate, with less of a positive impact or more of a negative impact, can now be considered. Additionally, with a good reputation built, it should become easier to get stakeholder buy-in from systems where the groups responsible for them were previously wary of IdM.

Good candidates would be a further data authority system (e.g. the HR system the SRS was integrated in the first phase), along with one or more data consuming systems that were not integrated in the first phase because of complexity or lack of stakeholder buy-in.

There should, however, be a note of caution sounded at this point. The success of the first phase of implementation, and the good reputation of IdM gained because of it, can be easily lost if this second phase is overly ambitious resulting in any perceived failures of integration. Do not get over-complacent about past successes.

7.5.3 Further targets

Given the successful integration of secondary targets, further phases of integration can be accomplished. These will likely be a rolling set of targets that change over time as an academic institution's systems are replaced over the course of years.

If the major sources of identity information are now integrated (such as the SRS and HR system), any remaining such systems should be integrated where possible, and all remaining data consuming systems should be integrated where the benefits of doing so outweigh the effort involved to do so.

7.6 Writing an IdM Roadmap

The sections above describe how to work out what needs to be done, and how to organise it into phases. The final task is to turn this information into a draft Roadmap for IdM at the institution. To do this, it must be remembered that a Roadmap is not a Project Plan; it is a higher level strategy document, indicating projects which can be designed to fulfil parts of the Roadmap. This means that the most difficult tasks which face the author of a Roadmap is to give a timetable and estimated cost for the implementation of its phases.

If there are existing Roadmaps for other planned activities in the Institution, it is essential to consult these to see how the document can fit successfully into the local culture. Authors of these documents are also likely to be able to give good advice.

Once drafted, it is sensible to circulate and discuss the roadmap. An appropriate body to use for this would be the IT Service Management committee, or equivalent. Clearly, it will not be prudent to suggest major changes to systems which are due to be replaced immediately afterwards.

The Roadmap as described here is basically a one-off document. As an alternative, it is well worth considering writing a Roadmap which is intended to be rolling document, describing the next year's work in considerable detail and outlining future phases to follow on from it, and then updating the Roadmap to reflect progress during this year.
7.6.1 Roadmap Sections and Layout

**Introduction**

This should contain a high-level overview of the importance of good IdM to the institution, and the purpose of the Roadmap (to give a practical overview of how to achieve high quality IdM, given its current status).

**Requirements (or Problem Statements)**

This section should describe what needs to be done (or, if couched in terms of Problem Statements, what issues need to be solved).

**Timetable**

Described in more detail below. This section should include estimated times for phases, with dates for key deliverables.

**Cost Estimates**

It is likely that at least part of the work in each phase will involve establishing the solutions to meet the requirements of that phase (e.g. to decide which IdM solution to purchase, if any), and that cost will be heavily dependent on these decisions. However, it should be possible to give a broad outline with a wide margin for error (e.g. “Phase 1 is expected to cost between £50,000 and £100,000”) and outline where the major costs are to be expected (e.g. in IT purchases and staff time), and when more accurate figures can be expected. Bear in mind that it is likely that any work will have to be carried out within a budget less than the maximum agreed at this point.

**Staff Involvement**

Outline which current institutional staff are likely to be involved, where their existing responsibilities will need to be covered, and where recruitment or use of consultants will prove desirable.

7.6.2 Roadmap Timetabling

Timetabling will consist mainly of slotting required tasks into each phase, and estimating how long each phase will take. As a general rule of thumb, each phase should last between 6 and 18 months; there may be local reasons to stick with a fairly rigid span for each phase (e.g. because matching a phase to a financial or academic year makes it easier administratively). If there are clearly related general institutional roadmaps already in existence, such as an IT Strategy roadmap, it will make sense to fit phases with the information in this and its update schedule.

As the Roadmap is going to include tasks which integrate different systems across the institution, the management team for each system will need to be consulted for timetabling work on it. They should also be able to help to estimate the time and cost of the type of changes that the Roadmap is proposing to make to these systems.

Each of the tasks listed for a phase would be a candidate for one or more IdM projects to carry out.

7.6.3 Example Outline IdM Roadmap Timetable

Phase 1 (18 months)

- Implement Central IdM systems and Identity Vault
- Integrate Student Records System as source of student identity information
- Implement manual system for managing identity information of other types of users
- Integrate network account creation and deletion system
- Integrate email account provisioning system
Phase 2 (12 months)
- Integrate HR system as a source of staff identity information
- Integrate VLE
- Integrate Identity card and physical access systems

Phase 3 (12 months)
- Integrate NHS staff database as a source of institutional NHS identity information
- Integrate alumni systems as a source of alumni identity information
- Integrate groupware systems (portal, wiki, blogs)

Further phases (6 months, time permitting)
- Identify any other applications and assess whether they should be integrated or not.

7.7 Conclusions
Establishing a roadmap for a measured, phased approach to implementing and maintaining an IdM system is vital if such a project is to be successful. Identifying which target systems should be integrated into the IdM system in which phase of implementation can be a major factor in this success, or in its failure. There are no concrete rules as to which systems, or types of systems are most appropriate; however, using the guidance provided should help an academic institution to make an informed choice and construct a roadmap that is suitable for their circumstances.
8 Ensuring Continuity of High Quality IdM

8.1 Introduction

Executive Summary
Work on Identity Management cannot stop once an institution has implemented high quality procedures and technical solutions. Institutional changes need to be reflected in the ongoing management of the policies and processes governing IdM.

Section Contents
- 8.1 Introduction: Why the long term profile of IdM matters
- 8.2 Politics and the Profile of Identity Management: The role of politics in IdM policy
- 8.3 Applying Identity Management Principles to New Initiatives: How to ensure technical and cultural changes do not undermine the quality of institutional IdM
- 8.4 User Communication: The importance of end user involvement in IdM

There are various issues which can conspire to bring about a return to small scale ad hoc processes which reduce security and accountability, which are discussed in this section along with approaches which are suggested to help prevent the balkanisation of IdM in the institution. Methods which can be used to combat this problem include keeping a high profile for IdM in the institution, understanding how to apply IdM principles to new initiatives in the institution, and ensuring that members of the institution know about the local and global aspects of IdM as they apply to their role within the institution.

Effectively, the IdM roadmap needs to evolve into an IdM strategy, with IdM an important part of other strategic initiatives within the institution, becoming an automatic consideration when new projects are devised – in both teaching and research, and in the support services which enable these front line activities. Every new research project, every new application or service made available to users, every departmental re-organisation: all will have a role for IdM, and all carry the possibility of failure to maintain a sufficiently high standard to ensure security and efficiency for members of the institution.

8.2 Politics and the Profile of Identity Management

There is an important political role in promoting high quality IdM in an FHEI. Compared to many commercial organisations, FHEIs are often relatively anarchic places, with less scope for successful imposition of rules from the top of the organisation. However, it is still the case that without support from senior management, IdM will not get a place on many agendas at all. The business case for high quality IdM has been discussed elsewhere in the toolkit, and is a clear starting point for any attempt to maintain the profile of IdM, especially as anyone to be convinced of the need to promote IdM good practise will need to be convinced of its benefits.

8.2.1 What Happens When Identity Management is not on the Agenda

Essentially, the benefits of IdM practice are lost, as those involved in projects and the setting up of new services improvise their own IdM solutions independent of official services and processes. This is not because the people doing this would be unwilling to link to the official IdM infrastructure, but because they either do not know that it can work with them or because they want to do something which the official IdM infrastructure does not quite do, and either don't realise this (and then go on to use a service for a purpose for which it was not intended) or don't know how or expect it to take too much effort to request changes in the services and processes to cope with new use cases (in which case they will invent their own, inefficient and potentially insecure, processes).

In the short term, connecting new projects and services with existing IdM processes and services may well take more work, especially if an external supplier has a product to sell which does not integrate with local
IdM systems. It is important, therefore, to have some mechanism for both checking that this does not happen and helping those in situations where they have to work with unfamiliar services and systems, especially when they are the interface between the institution and a supplier. In this sort of situation, it is important that potentially complex local IdM requirements are not suddenly brought into play late in the day, but are established as early as possible; and this is impossible unless IdM is on the agenda in the institutional culture.

8.2.2 The Need for an Identity Management Strategy

In an FHEI, there are large numbers of people who can at least start a need for new services or initiate new projects. Students can bring pressure for such initiatives as Bring Your Own Device. Members of academic staff may want to start collaborative research projects with external partners, each participant needing access to local services in the institution. Support staff may need to establish access to new external resources, or seek to streamline physical access controls by introducing new management software and associated hardware. Changes in the law governing some aspect of the institution’s activities may lead senior management to enforce change within the institution, requiring, for example, new access restrictions on personal data.

All of these changes have IdM implications which need to be managed, and those involved in implementing these changes are the principal individuals who need to be convinced that existing central IdM processes should be used or modified as appropriate. However, these people, at the sharp end of changes, are not the only people who need to understand the requirements of IdM good practice, as they will need to have the time and resources (which may well include time from other members of staff) to ensure that the new service or resource is integrated with existing systems and processes. This means that middle and senior management will need to be convinced as well, even though the actual knowledge they need will be less and of a rather different kind – business cases rather than technical details.

8.2.3 Formulating an Identity Management Strategy

To formalise the position of Identity Management in an institution, it is useful to produce an Identity Management Strategy. This will differ from the Roadmap because it does not have a specific, one-off target, but is designed to be a permanent and regularly updated document. The Strategy should start from where the Roadmap ends, on the assumption that most of the work described in the Roadmap has been carried out. But it will have similar aims (the promotion of good IdM practice) and a similar target audience, which means that the Roadmap would make a good starting point for development of the Strategy.

It may be considered appropriate for an IdM Strategy to be part of a more general strategic document, such as an IT Services Strategy. It should be remembered that the technical aspects are only a part of IdM, and that they are often easier to manage than the business processes and political aspects of IdM. IdM is also not restricted to a single department, but will be pervasive throughout the institution. For these reasons, it makes sense to have a separate IdM Strategy, unless the culture of the institution seems to fit better with the idea of one which is part of an existing strategic document.

The Strategy should be a document which is regularly re-examined (say, once a year) and which has an owning body which meets regularly. The non-IT components of IdM make a IT Services committee a poor choice for this, especially as doing so would exclude important stakeholders such as HR and student administration. The appropriate group should be a cross-departmental committee of middle management with strategic responsibility, chaired by an appropriate senior manager.

Introduction

This should contain:

- a high-level overview of the importance of good IdM to the institution (which can be based on the discussion in the Roadmap section of this Toolkit);
- a description of the purpose of the Strategy (the promotion of high quality IdM in the institution to users and managers);
- a summary of the situations to which it should be applied (as described in this section of the toolkit) would also be useful;
• information about who is responsible for the Strategy and its update schedule.

Identity Management at X

This is intended to set the context for the Strategy rather than to act as a main source of information about IdM. This section should describe:

• The context of IdM at the institution (e.g. legislative constraints, specific organisational constraints such as a collegiate structure or NHS involvement).

• The main systems and processes for IdM at the institution (abbreviated to X here), and link to more detailed documentation. Contact details could be included here. No more than one or two paragraphs should be written about each system described.

• How these main systems relate to one another. A simple diagram may be more useful than a verbal description.

Assurance

The purpose of this section is to describe how IdM quality is assured at the institution. It should include:

• Information on how IdM good practice should be applied to new projects and services, and is probably the most important section of the Strategy for its intended audience. The next part of this section gives an overview of the principles likely to be relevant.

• A description of the management structure surrounding IdM at the institution (overall responsibility, relevant committees, etc).

• A list of the major contractors involved in providing technical IdM systems in the institution.

Stakeholders in Identity Management Good Practice

The title of this section indicates that this is slightly different from a list of stakeholders in the strategy itself. The table below is an example which should help to devise a customised local stakeholder table.

<table>
<thead>
<tr>
<th>Stakeholder group</th>
<th>Relevance</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior management</td>
<td>Have the ultimate responsibility for IdM in the institution; concern for reputation of the institution; oversight of departments responsible for implementing strategy; responsibility for oversight of technical policies.</td>
<td>Medium/high</td>
</tr>
<tr>
<td>Middle management in non-technical departments</td>
<td>Desire to maintain efficiency and security; requirement to follow institutional standards</td>
<td>Medium/high</td>
</tr>
<tr>
<td>Middle management in technical departments</td>
<td>As preceding entry; responsibility for implementation and management of technical solutions to drive institutional IdM; responsibility for IT security; responsibility for development of technical policies.</td>
<td>High</td>
</tr>
<tr>
<td>Technical staff</td>
<td>Direct responsibility for technical solutions to drive IdM; responsibility for implementation of new services; responsibility for implementation of IT security; responsibility for content of technical policies.</td>
<td>High</td>
</tr>
<tr>
<td>Staff of Human Resources department</td>
<td>Direct responsibility for several of the business processes which manage the staff IdM lifecycle; responsibility for oversight of staff induction process.</td>
<td>High</td>
</tr>
<tr>
<td>Staff of student administration</td>
<td>Direct responsibility for several of the business processes which manage the student IdM lifecycle; responsibility for oversight of student</td>
<td>High</td>
</tr>
</tbody>
</table>
### Stakeholder Relevance

<table>
<thead>
<tr>
<th>Stakeholder group</th>
<th>Relevance</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>department</td>
<td>induction process.</td>
<td></td>
</tr>
<tr>
<td>Project managers /</td>
<td>Incorporation of IdM processes and technology directly into their work;</td>
<td>High</td>
</tr>
<tr>
<td>Business analysts</td>
<td>Interest in development of policies and processes in the institution.</td>
<td></td>
</tr>
<tr>
<td>Academic staff</td>
<td>Desire to spend time researching and teaching rather than carrying out</td>
<td>Medium/low</td>
</tr>
<tr>
<td></td>
<td>IdM functions; expectation of efficiency in management of research projects; interest as end user of institutional systems</td>
<td></td>
</tr>
<tr>
<td>Students</td>
<td>Desire to carry out study without encountering problems due to inadequate IdM; interest as end user of institutional systems; driving force behind adoption of many new technologies in the institution.</td>
<td>Low</td>
</tr>
</tbody>
</table>

### Responsibilities

This part of the Strategy is intended to show how the stakeholders identified in the previous section should act in order to quality of IdM at the institution is preserved. As with the stakeholder table itself, the following list is an example for customisation to the local situation.

<table>
<thead>
<tr>
<th>Stakeholder group</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior management</td>
<td>To ensure the recognition the importance of IdM good practice to the smooth running of the institution.</td>
</tr>
<tr>
<td>Middle management in non-technical departments</td>
<td>To ensure that relevant policies are followed; to ensure that new initiatives involve appropriate individuals who can advise on IdM good practice.</td>
</tr>
<tr>
<td>Middle management in technical departments</td>
<td>As preceding entry; To manage technical policies and procedures; to assign and organise training for individuals who can advise on IdM practice throughout the institution; to manage production of documentation regarding IdM.</td>
</tr>
<tr>
<td>Technical staff</td>
<td>To develop technical policies and procedures; to provide IdM good practice advice throughout the institution; to develop and maintain documentation regarding IdM.</td>
</tr>
<tr>
<td>Staff of Human Resources department</td>
<td>To develop and document the business processes which manage the staff IdM lifecycle, and the integration of these processes with other IdM processes in the institution.</td>
</tr>
<tr>
<td>Staff of student administration department</td>
<td>To develop and document the business processes which manage the student IdM lifecycle, and the integration of these processes with other IdM processes in the institution.</td>
</tr>
<tr>
<td>Project managers / Business analysts</td>
<td>To ensure that the agreed processes and appropriate technical solutions are followed in projects around the institution; to ensure that processes and technical solutions are efficient and secure.</td>
</tr>
<tr>
<td>Academic staff</td>
<td>To follow technical policies and procedures where relevant to their work; to discuss IdM with competent individuals before commencing projects with new requirements.</td>
</tr>
<tr>
<td>Students</td>
<td>To follow technical policies where relevant (e.g. in password management).</td>
</tr>
</tbody>
</table>
8.3 Applying Identity Management Principles to New Initiatives

As technology develops, and the roles of FHEIs evolve, the nature of IdM within the institution should also change. An institutional IdM Roadmap will need to develop to continue to be relevant. A large part of this work should be obvious, in that relevant new challenges to the institution are likely to be fairly widely discussed. However, it is important to undertake some analysis, even if at a fairly superficial level (e.g. during a meeting of the body which holds ownership of the IdM Strategy) to see what implications it has for IdM. In the main part, these are likely to be in three main areas: data management, privacy, and security. These are clearly related and will blur into each other for many developments; the way to think about them for this purpose is that data management is about storage of information and the related processes, privacy is about protecting the individual user, and security is about protecting the institution.

While it is possible to reduce the issues after the introduction of new developments, it is clearly better to influence the technology involved before the fact if possible. This can be done by:

- Ensuring that requirements in ITT documents include safeguards for security and privacy and only purchase systems which satisfy these requirements;
- Encouraging developers in house to include appropriate security and privacy safeguards in their software;
- Encouraging the development of APIs which have data security built in to their design;
- Designing policies and processes so that the introduction of new systems and services require thorough discussion of security and IdM requirements.

An example evaluation is discussed in a blog article evaluating the IdM implications of the consumerization of IT\(^2\)

8.3.1 Data Management Issues

The main question to ask when looking at how new developments will affect the institution's stored personal data is what new requirements there might be for use of that data. Likely answers include:

- all data required is already stored and can be used for the new purpose without modification
- the data required appears to be present, but some of the new uses for that data may amount to re-purposing which needs work to be done (e.g. because it requires the data at a point in the IdM lifecycle of an individual before it is currently generated)
- the data required appears to be present, but needs to be checked to ensure that the new use of the data fits with the purpose for which the data was collected in the first place, for all potential users of the system (this includes, for instance, ensuring that the reliability of the data is sufficient – if users can amend an attribute themselves without verification, and its reliability is now important, the attribute is not appropriate for use in this context without changes to existing practices)
- new data needs to be sourced and stored

8.3.2 Privacy Issues

Any new application or technology which makes use of user data has the potential to erode the privacy of those who begin to use the new system. Several principles should be applied to ameliorate the risks involved in this:

- Authentication should be federated single-sign-on whenever this is an architecture compatible with the service being offered by the system. Single-sign-on is clearly useful for usability, and federation means that the service can be extended beyond the institution (to partners, for example) and that access can be anonymised where this is compatible with the requirements of the service (see also below). The functionality of the system may require extra security which makes this impossible, or there may be other reasons why this is not appropriate, but federation and single-sign-on should always be considered and discussed.

\(^2\) http://theidentitytoolkit.wordpress.com/2012/08/02/identity-management-and-the-consumerization-of-it-services/
• No data should be accessed, stored, or created by the new system except where it is functionally necessary. Where user data is to be stored by the new system its relationship with other data around the institution should be clearly understood (to avoid issues such as access continuing to be provided to users who are no longer institutional members).

• Wherever possible, the user data should be anonymised, so that the system cannot identify a specific user. This can be carried out with pseudonymous identifiers which enable the identification of multiple uses of the system by the same individual. The institution will need to keep records which enable the tracing of a user when this is necessary, e.g. in cases of abuse of the system.

• The user should be given the option of approval of the use, transport, or storage of data as often as is compatible with usability of the system (e.g. each time a new data item is to be used, or at the commencement of new sessions).

8.3.3 Security Issues
This section deals with security as it relates to IdM, not in greater generality, though that should obviously also be a concern with any new system or business process. Again, several principles should be applied to ameliorate security risks relating to IdM:

• Any user data which is transferred across a network should be encrypted and/or travel over an encrypted connection. While it is common to think of this in terms of transfer across the public Internet, there also exists the possibility of attempts to obtain data from inside the institution (e.g. through compromised machines brought within firewalls).

• Any web based interactive application should use SSL with valid and verifiable security certificates.

• Sensitive data which is stored by the application, such as user passwords, should be encrypted. It would be better still not to store such information.

• Sensitive data should not be passed across the network or displayed unnecessarily. There are still in 2012 systems which email the user their passwords in clear-text or which will display the password in clear-text on the screen, both clear security hazards.

• User rights of access within the system should be carefully controlled, and the use of prompts for re-authentication should be considered for sensitive or unrecoverable actions (such as data deletion).

• The system should not permanently store data of its own without a good reason (e.g. to provide continuity between sessions). (This is because the stored data has the potential to become out of date or continue to allow access to a user whose association with the institution has expired.)

8.4 User Communication

8.4.1 Introduction
Involvement of users in IdM is important, because without it they can be the weak link in security, through bad practice or lack of understanding what an institution is providing for them. So it is important to educate users in the best ways to use the IdM provided for them, and how to avoid security pitfalls. Related to this is the potential for members of an institution to use self-service IdM tools, of which there are potentially many kinds which could be made available, but all of which need some level of understanding of what is going on behind the scenes to be used effectively. As with every form of communication with users, it is important that what an institution tells them about IdM is accurate, clear, and helpful.

Social engineering – that is, persuading people to do favours which they should not do for someone they may well not know very well – is an important tool in the arsenal of those who have a serious desire to break the security of a computer system. Without user education on such issues as the undesirability of sharing passwords, an organisation is defenceless against this form of attack.

8.4.2 User Education
Keeping members of the institution informed about how central IdM at the institution is important for continuing to provide high quality IdM. Without information, members will start to improvise services of their
own where the institution may well already offers such services (from setting up new facilities as part of research projects, to sharing of documents, to maintaining their own access control lists for items of equipment). This will eventually lead back to the chaotic situation where effort is duplicated and where services are offered which are insecure. There are basically two aspects to this kind of education: those which are institution specific, such as how to sponsor an associate member, and those which are general, such as how to choose a secure password.

Institution Specific Education

There are a variety of ways in which members of an institution interact with the institutional IdM processes. These include:

• being an end user of IdM, as one whose identity is managed (e.g. to gain access to the institutional network)
• being a consumer of IdM (e.g. as a developer wanting to add single-sign-on to an application being built)
• being a participant in IdM processes (e.g. as checking physical credentials such as a passport before assigning a userid)
• being an overseer of IdM (e.g. as the manager of MIS services)

Each of these relationships to the institution’s IdM requires knowledge of, and (a variable degree of) understanding of the processes which have been put in place centrally to ensure its security and efficiency. Providing this knowledge and understanding is the role of institution specific education about IdM. However, it is also the case that different methods of imparting the education are appropriate to those who have these relationships. For example, end users can be informed about specific rules when they try to carry out an action which they are not permitted to do for some reason (e.g. attempting to log on to a server with restricted access which does not include the user), while training sessions could help consumers of IdM to be aware of central services which they can use, how to do so, and who to go to with problems.

The biggest challenge with this form of user education is that it can be hard to reach existing members of the institution when changes are made to services, processes, or policies. This means that whenever changes are made to central IdM policy or technology, it is important to evaluate who is affected, how serious it will be if existing members are not fully informed before they basically find out for themselves (the risks of not communicating), and how best to communicate the changes to each affected group (including whether the update information can be rolled into other communication requirements for any related non-IdM changes). A communications strategy outlining these things therefore needs to be part of project plans for IdM projects.

Good practice in user education about IdM is essentially the same as that for communication with stakeholders in any business operation. The essentials of this are:

• Identify the stakeholders involved in the specific IdM change being considered correctly.
• Be clear on the aims of the communication exercise.
• Build trust with stakeholder groups (through competence, primarily, but also through openness and by demonstrating respect for the stakeholder). Accuracy in the information presented is vitally important.
• Listen to feedback from stakeholders before, during, and after the communications exercise (in a small scale project, the first two may not be appropriate).
• Act on the feedback as well as listening to it.
• Use a mixture of tailored methods to engage with stakeholders, where this is appropriate for the scale of the project.

Generic Education

Much of the information which institutions might wish to pass on to members is generic in nature, in that it will apply to members of organisations of comparable size to FHE institutions anywhere in the UK or around the world. This means that there are often very good resources already available on the Internet which can be used or adapted to impart such information to members, or which can help in the compilation of information
to use (e.g. by helping the compiler to be sure that their advice is good and comprehensive). This is a list of
some of the topics worth explaining to users with sample recommended resources.

- Password management and security [http://hitachi-id.com/password-manager/docs/password-
management-best-practices.html](http://hitachi-id.com/password-manager/docs/password-
management-best-practices.html)
- Device security and encryption [http://www.infosecurity-magazine.com/blog/2011/11/10/how-to-
manage-bring-your-own-device/451.aspx](http://www.infosecurity-magazine.com/blog/2011/11/10/how-to-
manage-bring-your-own-device/451.aspx)

Institutions are likely to already have documents covering the following topics, which may not have been
thought of as having IdM components:

- Rules and recommendations covering management of personal data (as a response to the Data 
  Protection Act)
- Accessing electronic resources
- Use of Eduroam

Additionally, many aspects of institution specific education will also include generic information; for example,
a briefing on an institutional VPN should include some generic discussion of the nature, purpose, and role of
virtual private networks.

### 8.4.3 Channels and Methods for User Education

Most FHEIs will already have mechanisms for communication with users, and these should be utilised for
user education in IdM. A wide variety of approaches and channels will be available, from presentations at
induction events to material on the IT Services support web pages to training courses to messages which
appear on login to the network. Each method will have specific advantages and disadvantages, which
depend somewhat on the institutional culture, and which will be familiar to members already. To give some
examples, induction events often attempt to impart overwhelming volumes of material, while on the other
hand technical support web pages will only be read if there is a perceived problem.

The solution is to use multiple channels, and to fit IdM material alongside and complementing other
information of interest to the user. It is sensible, for example, to including some information on password
security alongside mechanisms which make it possible to change the network password, or information
about accessing central IdM solutions in more general guidance for technicians and software developers.

### 8.4.4 Assessing the Impact of User Education

It is vital to measure the effectiveness of user education methods being used in an institution, to ensure both
that the information is reaching the people who need to receive it and that money and effort is not being
wasted on ineffective measures. A wide variety of methods can be used to make an assessment as to the
impact and success of user education initiatives. It can be possible to do so in the context of existing
information gathering exercises, such as surveys carried out to assess the work of IT Services which many
institutions carry out on an annual basis. As with the channels to use for user education, its impact is best
measured by additions to existing tools to gauge the satisfaction of institutional members for the services it
offers. For this reason, we will not give a list of possibilities here.

A more unusual method to determine user understanding of security issues is described in more detail in this
blog post[^29].

### 8.4.5 Self-service Identity Management

Many IdM systems have some form of self-service, where users can carry out tasks on their own behalf
without having to involve central IT services staff. Giving users some control over their own data frees up the
time of technicians who would otherwise need to make updates on behalf of users, though it can lead to
problems if too widespread as there is little control if any over the quality of the data when updates are
devolved in this way.

The integration of self-service consoles into a single portal, which can also be used for other services such as
finance (e.g. employee expense claims, student fee payments, library fine payments) and library

borrowing, is something which offers a unified interface which can be contextualised automatically to each user. This clearly improves usability, but at the cost of extra work to integrate services from disparate systems together.

Tasks with IdM aspects which are commonly made available for self-service include:

- password changes
- personal address management (for physical addresses, non-institutional phone numbers and email addresses)
- registration for courses (for students)
- application for membership on behalf of associate members of various types (usually restricted to staff, and possibly to subcategories of staff)
- making requests for access to services (typically requiring approval; identifying who can make requests and who should approve them is an important part of the analysis of IdM in the institution)

Many other changes to personal data are generally initiated by members, such as changes of name, department, or position, but are more likely to need to be carried out by IdM system managers. To extend it too far can be problematic, as would be the case where users can change their primary email address to one which is not an institutional address, without checks to ensure the validity and continuing use of the address, making email contact impossible when a user mistypes their home email or changes it. (This happened at at least one UK institution in between 2000 and 2010.)

As well as simplifying processes, self-service IdM encourages user involvement and provides an ideal channel for user education where it can be incorporated into help information and in checks made (e.g. by measures of password strength). All three of these are good reasons to adopt it for some processes, though a lack of full validation means that it is not appropriate for many types of data management.
9 Designing and Managing an Identity Management Project

9.1 Introduction

Executive Summary
This section deals with aspects of project management that may be particular to institutional work aiming to implement identity management facilities, including: Identifying the people to be involved in planning; Identifying the aims and scope of the project; Deciding on the approach to use; Integrating with non-IdM work; Assembling project plans and budgets. Common key institutional benefits of improved IdM are outlined for use in an institutional business case.

Section contents:
- 9.1 Introduction
- 9.2 The Key Benefits of Good Quality Institutional Identity Management: Three key benefits listed and explained
- 9.3 Designing an IdM Project: A discussion of project planning issues specific to IdM Projects
- 9.4 Putting together a business case: Guidance for the creation of a business case for an IdM Project
- 9.5 Managing an IdM Project: Issues specific to IdM Projects which affect how they can be managed
- 9.6 Appointing Staff to Manage IdM: Describes the posts of Information Security Manager/Officer and Identity Management System Manager, with example real world job specifications and descriptions

It is not possible for this Toolkit to offer a single business case, as institutional requirements and current positions will be very different, even if there are some gaps that are likely to be picked up by an audit. It is also the case that every organisation of the size of an FHEI will of necessity be carrying out IdM, so a business case for doing it is superfluous. This section describes, in general, how an IdM project could be designed and managed. It covers mainly those aspects of project management which are especially relevant to IdM work, rather than project management generally, which is covered by many books, articles and training courses. Institutions may have guidelines and policies covering project management (e.g. the use of frameworks based on PRINCE2 or other formal methodologies) which would be required background to the setting up of any project, not just an IdM project, and which cannot be covered here. This section will also not cover how to prioritise the different IdM projects which might be suggested by a Gap Analysis; this is covered by the IdM Roadmap section of the Toolkit.

The guidance given here is intended to be general enough to apply to IdM projects of any size, from small scale changes to data formats in an identity repository to the implementation of a central IdM system. Information specific to particular kinds of projects will be described in other sections of the Toolkit. No particular assumptions are made about the approach which is to be followed by the projects.

Similarly, the guidance here does not assume that the projects which are being designed are wholly, principally, or even tangentially technical IT work or, alternatively, concerned with business process management. Many IdM projects will be a mixture, and it should be remembered that implementing improvements to IT will not fix IdM issues where the underlying business processes are broken.

Key benefits from designing and managing internal projects to plug some known gaps in existing IdM processes will include:
- **Improved security**: Well designed, well understood, well documented and properly carried out IdM processes protect assets belonging to the institution.
- **Improved conformity with legal restraints**: Effective IdM processes will help prevent breaches of the Data Protection Act and of license agreements signed by the institution.
• **Improved efficiency**: Well organised IdM processes will prevent duplication of effort, and speed up processes such as user registration so minimising user frustration (e.g. with new staff members taking weeks to obtain working access to email). Well documented processes are easier to hand over to new staff, or to work with where the normal process management is unavailable. Well designed and properly implemented policies will ensure that management at all levels is able to obtain a good understanding of what the processes are and how they work. Projects which have IdM components (such as the introduction of new IT services which need to be integrated with an Authorisation Service) should be able to run much more smoothly.

This section will therefore suggest some generic components which can be used to produce a business case for an IdM project to fill a gap (or gaps) highlighted by a recently completed audit. By this point, it is assumed that an institution has carried out an audit or equivalent exercises to provide a gap analysis, so that there will be an individual or group of individuals with a good sense of where the gaps lie and what could be done about them. The content of this section will include both generic suggestions, effectively part of a business case for high quality IdM, and suggestions aimed at closing specific gaps and classes of gaps mentioned in the previous section. The audit report (and, if appropriate, information generated during the audit), together with the gap analysis, are likely to be vital sources of information for IdM related project design.

In particular, this means that no costings can be given, as the scope and nature of the project for which the business case is to be prepared is unknown.

It is also likely to be sensible to combine work on IdM improvements with other, related, tasks, such as enhancements to servers. This will often be necessary in any case, as security improvements may require software and configuration changes. In this case, the IdM enhancements should be included in a larger business case for the whole of the combined work, as this will tend to minimise risks and maximise benefits.

Managing change to business processes is often a difficult task, and when producing a business case for doing so, the author needs to be aware of potential difficulties which will be encountered. These tend to be political issues which are usually difficult to quantify in advance. Those who run processes may feel that they “own” them, and resent or fear changes made to them, and consciously or unconsciously sabotage projects which seek to alter the processes. Managers do not want to see crucial information moving out of the control of their team, particularly if their understanding of the replacement processes is kept vague. Those being assigned new processes may feel that they will now have too much work. These kinds of issues can only be solved by involving those who will be affected by change before the project begins: at the business case development stage, and by ensuring that all affected staff will be kept informed and/or involved throughout the proposed project.

The section ends with some guidance specific to particular types of IdM project, and a discussion of the appointment of staff to specific IdM management roles.

### 9.2 The Key Benefits of Good Quality Institutional Identity Management

9.2.1 Improved Security

Institutions have a duty to their members (staff, students) to manage data about them competently. This data itself has value, both to the member themselves and to the institution, and it can contain very sensitive information (such as bank account details). The value to the institution is such that it is impossible to function without it. Unauthorised access to, or loss of, or inaccuracies in, part of this data are all potential causes of problems with any process which uses this part. So it is vital that safeguards are in place to protect user data, both technical (e.g. the use of secure HTTP for authentication to web applications such as VLEs) and managerial (e.g. a procedure governing what information is permitted to be stored in mobile devices which may be stolen or mislaid off the institution premises). As the Privacy by Design report[^30], published in 2009 by the Information Commissioner's Office, puts it: "Organisations use identity techniques to bind personal information to the individual: good approaches deliver greater anonymity and privacy for the individual, whilst poor approaches collect, duplicate and expose personal information."

In addition to value in itself, user information is used to allow authorised access to other resources of value to the institution. This means that information made available to a third party could be used to gain

unauthorised access. Even where the actual credentials needed for access are not obtained by these third parties, the user attributes can often be used to obtain them (e.g. by providing information which can be used to guess poorly chosen passwords, or to persuade others to provide access when the third party poses as an individual who has lost their credentials through social engineering). Security breaches of this type will damage the reputation of the institution and may have legal consequences, as well as the direct losses which can be incurred when access is gained to physical and electronic resources (e.g. exam papers in preparation). Protecting sensitive user data is thus a form of insurance against potentially very serious security breaches.

9.2.2 Improved conformity with Legal Restraints

Institutions increasingly have legal constraints which regulate aspects of Identity Management. These are likely to include general legislative requirements such as the Data Protection Act, and requirements derived from agreements the institution has entered into such as resource licenses, federation membership agreements, partnerships etc. These will cover areas such as:

- how data is used
- publication of information about individuals (and when consent is required)
- accuracy of data about individuals
- prompt updating of data when necessary (including revocation of credentials when users are no longer entitled to hold them)

Clearly, it is essential for institutions to make their best efforts to comply with these constraints, and any work which is intended to improve IdM must as a matter of course look into what effect compliance will have on the desired outcome of a project. This should in turn mean that it is a priority to make sure that information on legal matters is available to those who might be designing and implementing IdM solutions; in some cases, such as with the multitude of resource licenses that an institution is likely to be a party to, this can be quite difficult in itself. It is likely to be useful to make an attempt to compile and maintain a list of known restrictions and access conditions which arise from sources such as resource licenses or Service Provider access conditions to help ensure compliance.

9.2.3 Improved Efficiency

Inefficient, poorly documented and duplicated business processes will be an unnecessary financial cost to the institution.

Loss of key members of staff who hold processes, policies and technical details in their heads is an unnecessary cause of disruption, which may have a high impact. Not only does it mean that their replacement needs to spend a great deal of valuable time working out how their predecessor carried out their tasks, but it leads to the invention of new processes, etc. designed in a hurry by someone not fully conversant with the institution and its idiosyncrasies. When a member of staff leaves, it is important to ensure that their job is documented, and if possible a hand-over period during which both the leaving staff member and their replacement are available (even if only electronically) is desirable.

Duplication of processes leads to wasted time and an increased potential for security problems. The latter is particularly likely to be the case if one of the processes is unofficial, and is carried out by someone lacking training in relevant subjects such as maintaining a data store securely.

Documentation is not enough to ensure high quality processes; there needs to be some assurance that the real life process matches (and continues to match) the documentation.

9.3 Designing an IdM Project

The following stages, most of which are going to be common to projects in any large organisation, may need to be passed through:

- Identifying the people to be involved in planning
- Identifying the aims and scope of the project
- Deciding on the approach to use
• Integrating with non-IdM work (if considered desirable)
• Putting together a project plan and budget
• Putting together a business case

This list is not necessarily chronological; indeed, the first four need to be at least considered more or less together as each will impact on the other three. The sensible way to approach this is to iterate through the first four until all those involved have common understanding of the basic project ideas, and then proceed to the business case, project plan, and budget.

Where there is an institutional roadmap for Identity Management, it is important that any IdM projects or project components are designed to fit in with the overall requirements of the roadmap; this will impact every one of these stages.

9.3.1 Identifying the people to be involved in planning

The list of common gaps in the gap analysis associates each with a set of stakeholders within the organisation. In many cases, this should immediately suggest the people to approach to be involved in the planning. Generally, it is likely to be essential to involve representatives from the departments involved in central IdM administration (IT Services, student registry, human resources, etc.). The seniority of the individuals that need to be involved will naturally depend somewhat on the institutional culture and the scale of the proposed project. This list is different from the list of those who will actually carry out the project, or who are needed at some stage of the project to provide input, feedback, or evaluation.

9.3.2 Identifying the aims and scope of the project

There are several questions which need to be answered here.

• Are there other known IdM issues which are closely related to the one(s) which prompted the project proposal which could sensibly be integrated? It is important to balance seizing the opportunity to kill two birds with one stone against the danger of weakening the focus of the project, which can lead to a lack of direction among project staff, as they work to different ends.

• How far should the proposed project go? It might make sense to only partially fill the gap(s) in some cases, e.g. where existing tools can be easily modified or new ones purchased to fix the majority of processes which fall in the gap, but other cases will be difficult to solve for practical or political reasons. Small scale quick wins are better than lengthy, convoluted projects which take a long time and may never produce the outputs expected of them.

• Is the project going to be policy led or practice led? This Toolkit and other related documents stress the importance of published policy documents. One approach which this suggests is to draft the policy where there is a gap first, and then adopt practice which fulfils the policy. (This runs the risk of impracticality.) The other approach would be to sort out the practice where there is a gap, and then draft a policy which describes the new practice. (This runs the risk that the policy never gets written as time on the project is spent fine tuning the process.)

• Will political difficulties need to be overcome or the institutional culture changed? Projects which need to do this are likely to be far more difficult to manage, and run a heightened risk of failure. Allowance must be made for this in planning the project, and it is important to discuss the strategy for achieving such goals as early as possible in the process. It is also likely that the culture, especially the resistance to change, will differ between different departments, and this will need to be taken into account when considering this aspect of the project planning.

9.3.3 Deciding on the approach to use

The approaches for an IdM project to improving the IdM in an institution can include the following, in approximate order of the scale of change involved:

• Installing a central identity management system and using this to replace or amend all existing IdM practices and bring them up to standard
• Outsourcing all or part of identity management to an external organisation
• Making ad hoc changes to existing systems to plug gaps
• Deciding that a gap is too insignificant/too expensive to fill and leaving the processes alone

Each of these has advantages and disadvantages, which are summarised briefly below. It is likely that any institution is likely to apply several of them, either to different processes or over differing timescales. Whatever approach is chosen, it is important that an institution creates a policy/strategy for identity management, and aims to converge to it over a set period of time.

<table>
<thead>
<tr>
<th>Method</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central identity management system</td>
<td>Makes tracking of identity management processes simple; There should be reasonable documentation/training available to ensure that processes are independent of (e.g.) staff retention; Problems may well have been ironed out by earlier users of the system</td>
<td>Expense; Integration with other systems (such as email, networking, etc.) may not be simple; The process of putting together an invitation to tender and evaluating responses to it may need to be extremely complex; Involves a major upheaval to existing systems and will not immediately be familiar to identity managers</td>
</tr>
<tr>
<td>Outsourcing identity management</td>
<td>It is no longer a problem that needs to concern the institution</td>
<td>Expense; Ensuring privacy when records are handled by individuals who have no direct contractual link with the institution (and may even be in different legal jurisdictions which have different views on privacy etc.); The process of putting together an invitation to tender and evaluating responses to it may need to be extremely complex</td>
</tr>
<tr>
<td>Ad hoc changes</td>
<td>Can be made over as long a period of time as necessary; Cheap; Gradual change means that most identity managers will be able to adapt easily</td>
<td>Political issues may inhibit necessary change (e.g. removal of autonomy from one department's IdM); New processes will need to be designed in-house and will not have been tested by others</td>
</tr>
<tr>
<td>Making no change</td>
<td>Zero immediate cost; No requirements to change familiar work practices</td>
<td>Hidden costs of unfixed problems may become very real in the future; Areas of legal non-compliance will not be fixed</td>
</tr>
</tbody>
</table>

It should be noted that making no change is only recommendable for minor gaps. The disadvantages of doing nothing are likely to greatly outweigh the advantages for other issues with IdM.

For an individual project, it is useful to score possible approaches for the following properties:

- **Difficulty**: difficulty of achieving target (as defined previously)
- **Risk**: level of risk of not doing anything
- **Measurability**: how easy it is to measure success: use of metrics as described in the Business Case section here is likely to be particularly important

### 9.3.4 Integrating with non-IdM work

Carrying out an IdM project may require non-IdM work to be carried out. In other cases, other work might well benefit from being tackled in the same project as fixing a gap. For example, extending single sign on to a VLE might fit in well with a planned upgrade to the VLE software. Many institutions have rigid timetables for changing mission critical software, in order to minimise disruption, so any IdM work on such tools may need to be scheduled to fit these timetables. Changing business processes is also likely to cause disruption and should be approached with similar care.

Additionally, the same staff are likely to be involved in both IdM and non-IdM of the work planned, as they will understand such matters as the existing software installation and configuration. This makes a single project
involving both strands more cost effective than two projects working on them separately; trying to work on multiple projects can lead to problems with time management for those involved, and the relationships between the work involved are unclear. To take the VLE example again, the addition of single sign on may require the installation of software patches which in turn require particular versions of underlying systems such as the web server, and this may be incompatible with the non-upgraded VLE software in unexpected ways.

9.3.5 Putting together a project plan and budget

- If the project manager is not experienced at working within the institution, it will be useful for them to talk through their plans with someone who is experienced at running internal projects, as they are likely to have useful structural, political, and financial insights, such as suggestions for useful people to involve in planning, potential sources of funding, etc.

- Thought should be given as to who will fund the work. IdM gaps such as those listed above may well involve several departments from different divisions of the institution, e.g. IT Services, Human Resources and an academic department. It may be possible to tie in some or all of the work with a related external funding opportunity, particularly if it can be argued that the work to be done is innovative.

- Many IdM projects will benefit from the inclusion of users to provide feedback from those who will be affected by the proposed changes. The term “users”, in this case, is not necessarily those who would be end users of IdM, such as students and teaching staff, but would include administrators of systems which are to be changed, or where the mode of operation of such systems will be changed as an outcome to the project. (And where this happens, integration of such changes needs to be considered as part of the project task list.) For example, changes to the user attributes stored in a repository are likely to affect other systems which consume these attributes, and which therefore will need to make changes to configuration or, more seriously, to the processes and software involved. (See also the discussion about Stakeholders in the business case section below).

- The planners need to decide how the project is to be structured. This includes how it should be divided into phases, a basic idea of how the work could be divided up between stakeholders, what the exit strategy should be for the project (e.g. who will maintain software installed during the project after it is completed?), whether and how users need to be involved, etc. Where there are political obstacles to overcome, a well documented pilot/testing phase with a friendly guinea pig group is likely to be advisable.

- Some institutions will have structural requirements for project proposals which are to be funded internally; this will also be true of any external funding bodies involved. Budget holders and senior managers who will be stakeholders in the planned project may also have (extra) requirements.

9.4 Putting together a business case

The discussion in this section is based on the summary of business case structure provided by the Office of Government Commerce (OGC) (no longer available). The various subsections outlined there for generic business cases are only listed here where there are specific IdM comments to add to the generic guidance in the document.

9.4.1 Strategic Fit

**Business Need**

The business need for high quality identity management - and thus to projects will fill gaps in identity management provision - can be based on the three key benefits associated with good IdM, which are likely to apply to some extent to any project aimed at increasing IdM quality.

For each of the common issues listed in the gap analysis, the follow business needs apply.
Lack of Commonality of Definition of "Identity Management"

Planning and management of projects which use IdM (which, in today's FHEI environment, a large proportion) is improved when those involved share an understanding of the meaning of IdM

Heterogeneity - Independent, Disparate Systems

Integration of systems (particularly to enable the removal of ad hoc processes) will in general improve security (in most cases) and will make IdM the responsibility of trained and experienced practitioners

Limited De-provisioning

Improvements in security, particularly gains in protection from unauthorised access by former members of the institution

Formal Procedures

These will make IdM processes easier to understand, and therefore improve efficiency, saving staff time and reducing errors

Common Standards and Central IdM Administration

Enables improved data reuse across the institution, together with improved security and efficiency

Identity Management Data Quality

Improved efficiency and reduction of errors affecting personal data for institution members and its use

Use of Non-unique User Credentials

Improved efficiency and accuracy, particularly in the revocation of credentials in a timely fashion

Policy of Reuse of Identifiers

Improved efficiency and accuracy

Contribution to key objectives

The business strategy and the IT/estates strategies identified in the Organisational overview section of the business case are likely to include targets, objectives and so on. The business case for an IdM project needs to point explicitly to those targets/objectives which it will help to achieve. Again, this Toolkit cannot offer generalised guidance here, but it should be borne in mind that IdM improvements combined with other work are likely to be stronger in this respect than either part of such a project considered separately.

Stakeholders

The following groups are likely to be stakeholders in most important IdM processes in any institution. When putting together the business case, the author needs to consider whether other groups in the institution should also be included; the listed types of stakeholders may well also require local modification.

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Interest</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Managers</td>
<td>Oversight of most of the institution's major, centralised IdM processes</td>
<td>High</td>
</tr>
<tr>
<td>Library staff</td>
<td>Access to electronic resources is one of the important ways in which identities are exposed beyond the institution</td>
<td>High</td>
</tr>
<tr>
<td>Staff in MIS, Registry, Human Resources and similar administrative departments</td>
<td>Oversight of much of the raw data managed by IdM processes</td>
<td>High</td>
</tr>
<tr>
<td>Senior management</td>
<td>Overall responsibility for IdM and public accountability for security/privacy lapses</td>
<td>Medium</td>
</tr>
<tr>
<td>Other staff and students / Applicants</td>
<td>Security and privacy in the handling of their personal</td>
<td>Low</td>
</tr>
</tbody>
</table>
### Stakeholder Interest Importance

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Interest</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>to job vacancies and for study</td>
<td>data</td>
<td></td>
</tr>
</tbody>
</table>

### Scope

The options for reduced scope or larger scale versions of a project will be dependent on the precise nature of the work being considered. It should be noted that many IdM changes are likely to be all or nothing, and that half-hearted attempts to change business process are more likely to increase confusion, inefficiency and the potential for security and privacy breaches than to reduce them.

There are always likely to be options which are rather more peripheral to the main aim of the project. For example, the project team could spend time researching the various software options available for IT projects, or the project could include or exclude extensive testing with users of the changed processes or updated software, or integration of more or fewer systems with the desired change, etc. Project designers should beware from including too many choices, but at the same time, some scope for choice is useful; it at least shows those who are considering whether the project should go ahead that the planners have considered other options. It should be clear what the issues relating to each option are; in particular, it is sensible to note where options could sensibly be delayed to a follow on project.

### Constraints

Again, the information that should be discussed in this section of the business case will depend on the individual institution and the specific project. The political issues mentioned above will be constraints, as will legal requirements listed in the gap analysis which govern aspects of how the institution can carry out IdM: general legal requirements such as the Data Protection Act, and (relevant) requirements from agreements the institution has entered into such as license agreements, federation membership agreements and so on. It is vital that project planners should consider how these general constraints might affect their project, as the consequences of not doing so can be severe.

### Dependencies

There are likely to be dependencies which are not IdM related and which would affect any institutional project, such as the availability (or recruitment) of staff. More specifically, IdM projects might require the completion of IT systems projects (e.g. updating software in use in the institution to a particular version), or planned changes to other aspects of the institution (e.g. work on physical security systems by the Estates department). There are no general dependencies for work on IdM processes.

### Strategic benefits

The principal strategic benefits of an IdM component of a project can be extrapolated from the business needs given above. They should be dovetailed with the strategic benefits of the other aspects of the project, where these exist. These should be linked to institutional strategic objectives wherever possible, so reference should be made to appropriate documents (such as IT Service or Library Strategic Plans) where these exist. If there is an institutional strategy for IdM, this should be referenced in any proposal for IdM work, with clear indications of which aspects of the strategy motivate the project under consideration and how it will help achieve goals from the strategy.

### Strategic risks

It is not possible to give an exhaustive list of general risks for IdM projects (for example, there may be specific risks associated with the fulfilment of IT requirements which are part of the project which are best evaluated by local experts). Where IdM change is a part of a larger project, there will also be risks which are not specific to IdM (and which may not even be related to IdM). However, some risks are common to many IdM projects.

*Political issues* These affect many projects which aim to change business practices, as most IdM work will. Typical problems which can occur include:

- individuals and departments are reluctant to change their working methods because more work will
be stressful or because less work makes them fear for their job

- individuals and departments are unwilling to cede "ownership" of and control over data
- people may be forced to work together who already have strained working relationships
- The "individuals" in this list could be either those who deal directly with IdM processes, or their management.

These issues are often hidden during the planning stages, but will lead to obstructive behaviour during the project itself, unless addressed during this process. Such obstruction can have a severe effect on a project, and if unchecked is quite likely to lead to non-completion.

Amelioration of this risk is generally likely to include involvement of all relevant individuals (both at management and junior levels) in the planning process, the obtaining of agreement (which may well need to be in writing) from management that the project is necessary and that they will support changes in their departments.

Technical issues Most IdM projects will have an IT component, and these will naturally carry the usual risks associated with IT (difficulties with contractors, software bugs, poor documentation, lack of training, etc.). Where IdM is involved, there are also potential issues with the data being processed, including:

- Data needs to be well understood before being re-purposed in any way (as described in the gap analysis)
- The data is often sensitive, so there are risks associated with exposure, including the temporary granting of access to contractors, if any. Data Protection Officers may need to be consulted about the risks involved in this area and the best ways to ameliorate them.

Awareness of these issues and good planning should enable them to be ameliorated.

The risks which are deemed relevant should be included in the risk register for the project, which should be kept up to date through the operational stages of the project.

Critical success factors

The success of IdM projects is to be measured in the adoption and use of the new systems and processes by the individuals within the institution for whom they are intended; there may also be opportunities to make specific measurements which would indicate success (e.g. a reduction in the number of IT Helpdesk queries relating to the IdM process involved). It is likely to be useful to include in the project recommendations that satisfaction with the new systems continues to be measured directly for a couple of years after the conclusion of the project as a whole, in particular for long enough to evaluate their resilience to the busy periods of an FHEI (new academic year and student intake, staff and student preoccupation during the exam season). While the way that this should be done is likely to be dependent on the specific nature of the project, methods which could be used include relevant objective metrics (such as the counts of related Helpdesk queries already mentioned), surveys of end users (e.g. by including relevant questions in annual surveys carried out by an IT Services department), the inclusion of questions in annual appraisals of those who carry out the IdM processes involved, etc.

9.4.2 Options appraisal

Long and short list of options

Clearly, the available options will depend heavily on the particular project. However, the IdM aspects are likely to have options related to those discussed in the gap analysis: make no change, make ad hoc changes (which should be spelled out for the specific IdM work under consideration), outsource, integrate with existing central IdM systems. Clearly, not all of these will be appropriate options to consider in every case, but it should be possible to adapt at least some of these into options to appraise with a SWOT analysis. The OGC recommends that a project as a whole should produce an options appraisal which "includes a do minimum option - at least two but no more than seven other options." As in the OGC document, some areas for consideration which might generate options are discussed in more detail below. See also the Scope section above.

31 http://en.wikipedia.org/wiki/SWOT_analysis
Opportunities for innovation and/or collaboration with others

Again, the contents of this section will be determined by the precise nature of the project. Approaches which are considered innovative will to a large extent depend on the institutional culture; e.g. some FHEI communities might find a suggestion to outsource IdM more controversial and unexpected than others.

Some aspects of IdM involve collaboration with others by their very nature; these would include management of individuals on courses shared between consortia of institutions, or the ways in which FHEIs and the NHS collaborate, or the reconciliation of different systems for IdM when institutions merge. But there may be other possibilities for collaboration in cases which do not immediately suggest it, such as the adoption of shared approaches to particular IdM tasks by several FHEIs, which are likely to make future collaboration on other activities simpler. It might also be possible to work with members of other institutions which have already carried out similar changes to those proposed in the project - though in this case there are likely to be costs involved which need to be justifiable in savings elsewhere: if a couple of days consultancy can be expected to save a week of project time, it is likely to be worth pursuing.

Service delivery options - who will deliver the project?

Options worth considering here include in house management and delivery (which may include options for such things as departments to involve in prototype testing of the new IdM system in the project); the use of consultants; external suppliers; working with other FHEIs. In many cases, these options could necessitate the discussion of how partners and/or suppliers would be chosen, managed, and their successful involvement measured. Where systems need to be maintained following the completion of the project, it is useful to indicate whether those who deliver these systems will continue to maintain them or whether this will become the responsibility of others (and if so how the transfer of control is to be handled); and how this requirement can be costed in the longer term. IT departments in particular have in the past tended to add new responsibilities to individuals without considering how they can be fitted into already full workloads, which means that tasks are neglected unless there is a critical reason why they need to be carried out.

Detailed options appraisal

This Toolkit should not prescribe any particular method to take for the calculation of costs and benefits. However, the key benefits of IdM improvements carried out as part of a project are likely to be 'soft' benefits, which do not have a direct financial value, so the method used to calculate the benefits of the various options should make it possible for such benefits to be taken into account.

9.4.3 Affordability

Budget costs will naturally be determined by the project as a whole. However, one note in the OGC document is particularly relevant in projects where IdM changes are proposed: "Note that savings or benefits achieved in one part of the organisation may add to costs elsewhere in the organisation or delivery chain. This is especially significant where the organisation has to maintain parallel channels for service delivery." In most cases, IdM business process changes will have the aim of reducing such parallel channels, but there may well be a need to maintain legacy methods for a period following the project completion.

9.4.4 Achievability

Similar Projects

It is not just possible but quite likely that other UK FHEIs will have carried out similar work to any proposed IdM business process changes. However, it may be more difficult to discover which FHEIs might be approachable, since organisations are generally unlikely to widely publicise failings in their existing processes. Where vendor provided solutions are involved, the vendor should be able to provide confidential references to other users of the solution.

Project roles

These will be determined by the nature of the specific project. Where business process changes are being made, it is sensible to seek involvement from as many stakeholders as possible, due to the potential risks
Procurement Strategy / Project Plan / Contract Management / Benefits Realisation Plan / PIRs and PER / Contingency Plan

This will be determined by the nature of the project as a whole. However, Post Implementation Reviews are likely to be very useful in projects involving IdM, and it is suggested that repetition of relevant parts of the audit may be an excellent way to carry out such a review.

9.5 Managing an IdM Project

Once designed, an IdM project is likely to require similar management skills to any project. The major difference from work supervised by the project manager in the past (assuming that they are experienced in project management) is likely to be that the tasks involved will combine business process engineering with IT, and this is comparatively unusual. However, the design of the project is likely to have established the timetable, budget, risks, etc., and it is only the political elements which are likely to de-rail the process. This factor makes it unlikely that an inexperienced manager will succeed, except possibly in very small scale projects.

9.5.1 Designing and Implementing IdM Processes and Procedures

The political difficulties which are associated with IdM projects generally will be especially strong for those aiming to design and implement processes and procedures - to re-engineer existing business processes, in other words. Involvement of interested parties is key here, along with (wherever possible) reassurance that the change is not going to lead to job cuts but should instead free up individuals to concentrate on the more interesting parts of their work.

9.5.2 Implementing a Central IdM Infrastructure

In this case, the scale of the project becomes the principal feature which needs to be managed. Disruption should be kept to a minimum, and the project should be scoped as narrowly as possible. For example, there are dangers associated with a big bang approach in which every process within the institution needs to be changed to use the new central infrastructure for IdM at the same time. It makes more sense to make the detailed changes to other processes in small steps, starting with a few representative processes and systems which can be integrated with the new central infrastructure in order to test that everything is in place. For some processes, it is of course sensible to consider running dummy versions: this will almost certainly be advisable for the testing of procedures concerning the registration of new students in the autumn.

9.5.3 Extending IdM to New Systems and Processes

Generally, this type of IdM project is likely to be relatively trouble free. It is also the most likely to be integral with other work on the system involved (and may well be required to be, if, for example, it is a software installation which has an update cycle managed by the institution to minimise downtime and disruption). The concerns which need to be addressed are discussed elsewhere in the Toolkit.

9.6 Appointing Staff to Manage IdM

It is likely that an institution will need to carry out several projects relating to IdM or that management will be needed to run central IdM systems which were not in existence or were not prominent beforehand. There are several roles which it may be appropriate to create, depending on the local circumstances.

9.6.1 Information Security Manager/Officer

This is a strategic post within the institution. The purpose is to mitigate risk within the institution relating to information, with respect to:

- confidentiality

108 of 123
• integrity
• availability

Since IdM will relate to each of these aspects of information management, the post holder will have a significant interest in work on institutional IdM. The post combines technical input into IT developments (in particular relating to ISO 27000\(^2\)) with non-technical help on information risk management. A real world example job description and person specification is available from the online Toolkit\(^5\) (with institutional identifiers redacted).

9.6.2 Identity Management System Manager

If a central IdM system is installed, then a permanent post should be established to manage it. The postholder will act to ensure reliable operation and continued enhancement to the system, in accordance with the roadmap or other relevant strategy documents and with guidance from (a group of) the IdM stakeholders who have already been mentioned in this section. A real world example job description and person specification is available from the online Toolkit\(^5\) (with institutional identifiers redacted).

\(^{109}\) of 123

32 [http://www.27000.org/](http://www.27000.org/)
10 Selecting Supplier Solutions for Identity Management

10.1 Introduction

Executive Summary

Where commercial procurement of systems or components is required, this section aims to help understand the IdM system solutions available, produce procurement criteria, and construct tender documents. Issues of product capability, technical fit and vendor suitability are considered; and advice is given on specific aspects of a tendering process and phased implementation.

Section contents:

- 10.1 Introduction
- 10.2 IdM System Solutions: Summarises the capabilities of modern IdM Systems and the considerations to use in making a choice
- 10.3 Tendering: How to tender for quotations for an IdM System
- 10.4 Example IdM Tender invitation
- 10.5 Conclusion

Once an academic institution has developed a programme of IdM work, and constructed a realistic roadmap for the work, the next step may be procurement of systems to achieve the initial goals of the roadmap. This section is designed to help academic institutions understand the IdM system solutions available, produce procurement criteria, and construct tender documents.

The IdM roadmap should inform several aspects of the process of choosing an appropriate solution for the institution. It should:

- Indicate whether the preferred IdM architecture involves a central IdM system or working to integrate existing systems which handle parts of the IdM requirements of the institution (such as the Student Record System, the software used by HR and the finance department, and the mechanisms used to create accounts on various systems).
- Indicate how the IdM work that the institution is planning should be prioritised.
- Indicate general requirements for software solutions which need to be developed or obtained from a third party (whether a vendor or an open source development consortium).

The roadmap will be a top level solution, giving strategic information. The process which went into developing the roadmap, which may include a detailed IdM audit, will have produced more detailed analysis which should make it possible to turn the general requirements which can be seen in the roadmap into a collection of detailed requirements as would be appropriate for an ITT document or project plan (as appropriate).

10.2 IdM System Solutions

An IdM system solution aims to sit at the heart of the academic institutions, connected to each IT system, responsible for both various aspects of overall identity and account management and the connections into each IT system to manage their integration into this wider identity-driven ecosystem. This section refers to an "IdM System Solution" because a comprehensive IdM implementation is very unlikely to involve a single product, technology, or service. It will instead be an amalgam of various related elements that combine together to fulfil the IdM requirements of the academic institution. Which elements to use - and which products to chose that perform the tasks of that particular elements - may vary wildly between academic institutions based on their individual needs.
10.2.1 Capabilities of an IdM Solution

While IdM implementations may vary wildly between academic institution, the whole solution of each will usually include at least the following main features:

- A central repository of identities and related identity information;
- Synchronisation mechanisms to various applications - to be able to “talk” in multiple protocols or languages to a variety of applications, enabling the gathering and publishing of identity information;
- Account provisioning/de-provisioning abilities - to control access for individuals within connected IT systems by provisioning/de-provisioning accounts within these systems and by managing those accounts' rights based on identity information.

These features provide the core functionality required of an IdM system solution. Beyond these, many other features are often seen. These may include, but are by no means limited to:

- Auditing - to provide comprehensive change history;
- Directory - to use as an Authentication back-end and to supply attributes used for Authorisation.
- Federated Identity Provider - to enable authentication and authorisation to remote services via federated means (e.g. using SAML);
- Group Management - to enable automated and/or manual placement of users into groups (useful for authorisation decisions);
- Identity reconciliation - automated and/or manual mechanisms for taking existing accounts from multiple IT systems and identifying, to a certain degree of probability, that those accounts belong to a single individual and linking them within the central identity repository;
- Password management - to enable password synchronisation between IT systems, enforce global password policy across these systems, etc;
- Self service portals - to allow individuals to update their information without the need of going through a central administration point;
- Shared Authentication Service - to allow seamless access to a variety of systems with a single credential;
- Workflow - to allow change requests of various natures to be submitted, validated, verified and approved by specified authorised personnel, and automatically actioned.

10.2.2 IdM Products

Many products are available in the marketplace that offer the core functionality of an IdM System Solution as outlined above, along with many of the other features discussed. Some examples of these products are those available from large well-known vendors - such as CA, IBM, Microsoft, Novell, and Oracle - and those from more specialised players such as Courion, Avatier, and many others. Sources such as Gartner can help identify these available products.

Many products from the larger vendors exist as a part of a vertical stack of applications that together provide most or all features potentially required for IdM, security management, legal compliance, auditing, single sign on, and a host of other related features.

A general comparison between IdM products is not feasible - genuine informed comparisons can only be drawn given a specific set of circumstances to calculate which is the most appropriate. However, some technical considerations for comparing IdM products and some general considerations to take account of when choosing the correct product for an academic institution can be detailed, and are presented next. Additionally, some of the questions presented in the Identity Management Policy Checklist Appendix may be of use in this task.

Assessing Capabilities of IdM Products

Individual IdM products designed to offer the core functionality of an IdM System Solution can do this in many different ways. Outlined next are a series of technical tasks that each available IdM product may or
may not be able to perform. To assess the suitability of a particular IdM product for a given circumstance, the importance of each of these areas should be assessed by the academic institution and each product under investigation should be evaluated given their ability to perform these tasks and the importance assigned by the academic institution to those tasks. The product that can achieve the largest majority of these could well be the most suited to that particular circumstance.

1. Data connectivity
   i. Able to connect to database, directories, files, and/or web services using well defined protocols to for data flows in and out;
   ii. Has a well defined API to enable custom developed connectivity to proprietary data sources for data flows in and out;

2. Data synchronisation
   i. Able to expose listeners to accept notification of deltas from source systems;
   ii. Able to poll source systems;
   iii. Able to publish data synchronously or asynchronously as single records;
   iv. Able to publish data asynchronously in batches;
   v. Able to maintain local queues for asynchronous data publications;
   vi. Able to use multiple threads for data subscriptions and publications where advantageous (e.g. where operations are slow, but many can be executed in parallel);
   vii. Support for one-to-many object relationships between systems;

3. Model
   i. Able to work in point-to-point mode with no persistent data storage except data source and destination;
   ii. Able to work in hub-and-spoke mode with central consolidated data store;

4. Data matching/de-duplication
   i. Able to match data between systems using simple multi-attribute exact matches;
   ii. Able to match data between systems using “fuzzy” match algorithms such as Soundex/Metaphone and Lievenstein;
   iii. Able to identity possible matches for human intervention and supports a workflow that enables this;
   iv. Support for record merges;

5. Data transformation
   i. Able to apply business rules with no reference to outside data using simple if-then-else logic (e.g. XSLT);
   ii. Able to apply business rules with reference to outside data using simple if-then-else logic (e.g. XSLT);
   iii. Able to apply business rules with no reference to outside data using high performance rules engine;
   iv. Able to apply business rules with reference to outside data using high performance rules engine;

6. Authentication
   i. Able to use local authentication methods for data sources and destinations;
   ii. Able to use federated authentication methods for data sources and destinations;

7. Audit and reporting
   i. Able to audit and store details of all activity;
   ii. Able to produce reports summarising specific activities and deliver them to appropriate
parties;

8. Governance
   i. Able to integrate with SOA governance in an existing SOA architecture

### 10.2.3 General IdM Software Considerations

There are also many general aspects relating to IdM products that should be considered when performing a comparative evaluation of them. This section highlights some of these aspects.

**Technical Appropriateness**

*Consideration:* Different IdM products have different technical capabilities, and different levels of completeness and complexity around each technical capability. Choosing an IdM product that does not fulfil the requirements of the academic institution, as defined in the IdM workplan and roadmap, could severely hinder the success of an IdM implementation.

*Mitigation:* Take great care when choosing an IdM product, making sure that it fits the technical and organisational requirements – with an eye to the potential future needs of the academic institution. Sources such as Gartner can be used to help understand the products in the market place, however, it is unlikely that anyone in within an academic institution has good enough real-world knowledge of each of the wide range of IdM products available to make an informed decisions. If this is the case then external consultants specialising in IdM implementations may be required.

**Cost**

*Consideration:* Different IdM products have different costs, and different costing models used. Choosing an IdM product whose cost does not fit within the IdM project's budget – including potential ongoing and future costs – could severely hinder the success of an IdM implementation.

*Mitigation:* Take great care when calculating the projected costs of an IdM product, making sure that the costing model in use is correct (e.g. per seat licensing vs per server licensing). Many vendors offer academic pricing options that are better value than standard commercial rates. Keep an eye to the potential future needs of the academic institution – e.g. if a per seat licensing mode is in use, plan for an increasing cost if the organisation grows.

**Flexibility**

*Consideration:* Any organisation – especially an academic institution – is likely to have various individual requirements and systems it wishes to connect to an IdM system. Each of these systems may require a different method of connection to the IdM system, and may place individual requirements on it. Some example of this might include:

- how users are mapped from the back end system to the IdM system – some systems may store an IdM-generated unique identifier internally, linked to a set of local credentials, other may be provisioned directly from the IdM system;
- how synchronisation between the backed system and IdM system – some may be able to accept “push” IdM messages via an Enterprise Service Bus or similar mechanism, some may “pull” IdM changes at regular intervals;
- how operations are performed – some systems may delete accounts by physically removing them from the system, some may mark them as inactive, while some may place them in a special container.

*Mitigation:* IdM systems with a demonstrated flexibility to handle any requirements made of it are better than those with less flexibility. At a minimum, any IdM system should obviously be flexible enough to meet the current needs of the organisation, however, any flexibility beyond this will help the IdM system adapt to future requirements made of it.
**Maturity**

**Consideration:** A wide range of IdM software is currently on the marketplace; some have been actively developed and available for several years, while some are much more recent entries. While newly developed IdM software may well be technically adequate, only time in the marketplace will demonstrate the capabilities and stability of such software.

**Mitigation:** IdM software with an established track record of successful implementations are more likely to be successfully implemented within an academic institution. Sources such as Gartner and industry reviews can help with assessment of the maturity of IdM software.

**Scalability**

**Consideration:** Given the tendency for academic institutions to merge, de-merge, shift focus, change direction, add new systems, replace or remove existing systems, etc – i.e. generally not staying in any stable state for any lengthy period of time – then requirements for the scale of an IdM system may drastically change over time. An IdM system that may perfectly adequately handle the current size and scale of an institution may or may not be able to scale to cope with future demands made of it.

**Mitigation:** Any proposed IdM system should be able to scale well (with additional hardware as required) to cope with an increase in both users and systems that it should be able to handle. It is not possible to advise upon a general specific figure for this, essentially, assurances should be sought that the number of users and systems it will handle in its initial implementation is not near the maximum figure that it is capable of handling.

**Security**

**Consideration:** An IdM system sitting at the core of many of an academic institution's systems and processes is a core part of the institution's infrastructure. It may well be handling and/or controlling a large amount of personal information about members and affiliates of that institution, and directly or indirectly controlling provisioning of user accounts on many internal systems. Thus, the IdM system itself needs to be protected and made secure, and all communications between systems should happen in a secure protected manner.

In practice, this means that it should be locked down and implementation of internal access controls and encryptions to limit the risk of unauthorized activity.

**Mitigation:** Any proposed IdM system should be highly secured, with comprehensive access controls. Encryption should be used where necessary to protect data from unauthorised access.

**Data Storage (and the Cloud)**

**Consideration:** Several vendors are introducing cloud storage for user data into their products. This is likely to provide convenience and lessens reliance on the security knowledge of the in-house IT team, but introduces other concerns, including:

- Storage of data in the cloud may mean that it is not in the same legal jurisdiction as the institution, and care must be taken with relevant legal differences (e.g. those between EU and US privacy regimes).
- Intermittent connectivity issues may prevent access to the data, impairing the functionality of the system.
- The institution will need to place a great deal of trust in the vendor's security and privacy systems.

**Mitigation:** Careful consideration needs to be made before taking the step of moving to the cloud, and the issues need to be discussed in detail with the vendor before going ahead. Some products allow the adoption of a piecemeal approach, with data sorted locally by the institution, in the cloud, or in a mixed environment. This may enable a small scale trial of the use of the cloud before committing the institution more fully.

**Outsourced/Third Party Identity Management (Identity as a Service)**

**Consideration:** There are now various companies which will carry out some aspects of IdM on your behalf. In the UK HE sector, this is most commonly used to pass on the effort of maintaining an Identity Provider for
membership of the UK Access Management Federation: the institution continues to manage the identity lifecycle of their members, but configuration and management of the IdP to use these identities for resource access is devolved. (See the JISC Guide on this subject for more details.) More generally, outsourced identity management providers offer authentication (typically using a federated architecture) and provisioning. Many of them are oriented to the commercial market, and effectively aim to link users to multiple Software as a Service providers.

In the more general situation, the usual means by which IdM is offered by third parties, known as Identity as a Service (IdAAS), is through the cloud, so the considerations above on use of the cloud also apply here. The additional potential benefits here are that outsourcing the work of installing, managing, and maintaining an IdM system frees up resources at the institution, saving time and money. IdAAS is also touted as a potential solution to the issues surrounding BYOD initiatives, by . Issues which may lead to difficulties with IdAAS include the difficulty of connecting the services to existing legacy systems as well as those already mentioned for cloud services.

Mitigation: The institution will still need to be responsible for managing the relationship with the supplier of their IdM services, and will need to be especially careful in this regard because of the sensitivity of IdM. It is also important to understand the differences between the FHEI environment and the typical corporate world, which will be more familiar to many vendors. Careful planning is necessary before outsourcing any aspect of the institution's operation which is as sensitive as IdM.

Open Source Identity Management Systems

Consideration: Many components of an Identity Management system can be realised with open source software, and some commonly are: directories and single-sign-on software in particular. Some vendors of Identity Management software also make open source versions of their products available, typically with reduced functionality. Open source software is particularly suited to an ad hoc, piecemeal approach to IdM, as described in section 8.3.3, Deciding Which Approach to Use, as components can easily be added when needed. With sufficient in house technical expertise, open source can also be easier and cheaper to integrate with other systems already in use. There are also now full scale open source IdM systems available.

However, the potential issues with open source software are also well known. There is often no guaranteed support (though informal support from user communities and developers is often usually very quick and helpful). There is no guarantee that the developers will continue to work on the product (though this is also a problem with commercial products, where the vendor could go out of business or change its focus). Its use can be difficult to sell to senior management, who expect software to be obtained through a traditional customer-vendor relationship, particularly with the expectation that an ITT is produced and answered by interested vendors. Internal technical expertise is needed for installation, configuration and management, which offsets the zero cost of the software itself (though there can be other benefits to the institution from having such expertise available).

Mitigation: Discussion with individuals knowledgeable about open source and in particular specific products can help allay fears. The JISC OSSWatch service will be a useful resource for this. Consultants are available to install and support many of the better known open source software products.

10.2.4 Vendor Considerations

There are several aspects relating to vendors who may bid on a tender issued by an academic institution. This section highlights some of these aspects that should be considered when selecting an appropriate vendor. Note that some of these are very similar to the considerations discussed around the vendor of the IdM products as previously discussed, since many of the issues are similar in nature.

Existing Academic Customer Base

Consideration: An IdM system within an academic institution can be vastly more complex and its implementation more troublesome than in the majority of standard business organisations, due to the very nature of such organisations. The user base is likely to be far more varied and existing systems that need integration with IdM unlike anything in the business world (student record systems, for example).

36 http://www.oss-watch.ac.uk/
Mitigation: Vendors with prior experience of implementing an IdM system in the academic world are more likely to be able to successfully complete an IdM implementation on-time and on-budget than those with no experience in this area. Therefore request potential vendors to provide references from existing academic customers.

**Partners**

Consideration: IdM systems must connect to, and interoperate with, many different types of systems from many different vendors.

Mitigation: Vendors with official partnerships with vendors of the systems already in place within an academic institution may help make supported integration between these pieces of software substantially easier, since they will have more experience of such integration, and access to direct support from those system's vendors. Given the range of software likely in place at any academic institution, more specifically it can be said that official partnerships or established relationships between the IdM software vendor and the provider of the academic institution's HR, Student Records, and helpdesk software will substantially ease implementation and migration difficulties inherent in an IdM project.

**Vendor Stability**

Consideration: Any full scale IdM implementation within an academic institution is likely to be a long and gradual process, and once implemented, will form a key business system for years to come. The collapse of the vendor of the IdM software, or the discontinuation of development and support for that software, could hamper the long-term viability of any IdM implementation using that IdM software.

Mitigation: Vendors of the IdM software that have a proven track record of financial stability are much more likely to be able to provide support, guidance, and development of the IdM system implemented in future years. Attempt to assess the stability of vendors. Sources such as Gartner can provide a major help with this assessment.

**Support**

Consideration: Unless the academic institution has a large amount of in-house experience with the various aspects of IdM that exist, then it will be at least partially reliant on vendor support for both implementation and maintenance of the IdM system. Any failures in support channels, or in appropriateness of support provided, could provide a major hurdle to any IdM project.

Mitigation: Vendors who can offer comprehensive support, both with the initial implementation of IdM software and with subsequent changes necessary as systems and procedural requirements changes, will enable an IdM project to achieve long term success. Those who are willing to provide support for bespoke solutions to specific problems, rather than official "out of the box" solutions only, will enable a greater degree of flexibility within an IdM system.

**10.3 Tendering**

Given the highly specialised knowledge often required when implementing IdM system solutions and their connection to existing applications, the detailed analysis, specifications, and technical implementation of many large IdM implementation projects is often procured externally from the academic institution itself. This section provides some help and guidance around how this procurement could happen.

**10.3.1 Procurement Regulations**

Since an IdM system is such a fundamental and far reaching system, any procurement is likely to be on a not-insubstantial scale. Since academic institution are generally public sector bodies, then various parts of EU procurement law may come into play. Academic institutions will need to ensure they abide by these laws at all stages.

**10.3.2 Budget**

The implementation of an IdM system can be a long term process made of many disparate projects, each
with their own requirements and budget. The initial project, however, should have a fully defined budget from its very beginning.

When calculating a budget, do not forget to make sure that each of the following items are included:

- Software licenses for all components of the IdM system;
- Annual support licenses for all components of the IdM system that are required;
- Operating system licenses;
- Hardware to run the software on;
- Implementation costs – whether external consultancy or internal costs;
- On-going Maintenance costs – whether external consultancy or internal costs;
- Internal Resources – project management, tender evaluation, implementation and maintenance;
- Training for staff – both in how to administer and how to use the system.

10.3.3 Phases of Implementation

There are many possible approaches to the organisation of the implementation of an IdM system. Which approach is used, and how it is used, will depend on what best fits the academic institution, circumstances, and budget.

Essentially, the implementation of an IdM system can conceptually be split into two separate phases:

Phase One – The drawing up of a detailed specification of hardware and software required, and a detailed project plan for implementing these;

Phase Two – The actual implementation of the system(s) detailed in Phase one, including testing, documentation, and migration of existing data.

One recommended implementation possibility is that of using a two phased approach, where each phase matches the conceptually disparate phases detailed above. Each of these phases, and how they can be organised, are discussed next.

Phase One

Phase One of an IdM implementation would consist of preparing a detailed specification for a system (or systems). This will include:

- A list of systems that should be connected to the IdM system;
- Details of all dataflows between all connected systems and the IdM system;
- A list of processes that the IdM system will take over;
- Hardware and software requirements (including number of licenses required);
- A statement of costs (software, consultancy, contracting) that would be required to deliver, test and document the specified system(s);
- A statement of the expected effort required from the academic institution's technical staff;
- An initial project plan for building the specified systems and migrating existing data;
- A test and acceptance plan;
- The options and costs for long-term support and maintenance of the system.

Phase Two

Phase Two of an IdM implementation would consist of the actual implementation, documentation and testing of the system(s) specified in Phase A. This would also include migration of existing data from legacy systems.
10.3.4 Organising phases

Given the separation of IdM implementation into two phases, there are a few options around how these can be organised. Each is explored in turn.

Both Phases Internally

In this option, an institution would carry out both phases of implementation in-house. The obvious advantages of this approach are the savings in external consultancy fees, and the in-house detailed knowledge of the implemented systems. However, any institution planning on doing this will need a great degree of experience in IdM system solutions, in order to be able to choose appropriate technologies, and a great degree of experience in implementing these systems, so as not to encounter common pitfalls needlessly. Also, do not underestimate the resources required to do either phase.

Phase A Internally, Phase B Externally

In this option, an institution would carry out the initial phase of detailing hardware and software required, and producing a project plan. This would then be used to create an ITT for the actual implementation. The obvious advantages of this approach are the savings in external consultancy fees, and the in-house detailed knowledge of the overall design of the implemented systems. However, any institution planning on doing this will need a great degree of experience in IdM system solutions, in order to be able to choose appropriate technologies. Also, do not underestimate the resources required to perform this phase.

Both Phases Externally as separate ITTs

In this option, an academic institution would issue a first ITT for an external company to come in and carry out the initial phase of detailing hardware and software required, and producing a project plan. This would then be used to create an ITT for the actual implementation, which would be issued as a second ITT. The same company may or may not win both tenders and carry out each phase of work. The advantages of this approach are that separate external contractors specialising in the intricacies of each phase of work could be used, little in-house expertise in implementing IdM systems is required, and that if the institution is not happy with the output of Phase One they are not legally required to continue to Phase Two. However, two separate ITT processes will require a great deal of administrative effort, an appropriate budget, and will leave the academic institution with little internal knowledge around the implementation process.

Both Phases Externally as one ITT

In this option, an institution would issue a single ITT for both phases, where the two phases would be separate items of work, and phase B would be specified to go ahead only if the institution decides that it is happy to do so. The advantages of this approach are that little in-house expertise in implementing IdM systems is required, and that if the institution is not happy with the output of Phase One they are not legally required to continue to Phase Two. However, this will leave the institution with little internal knowledge around the implementation process.

10.4 Example IdM Tender invitation

Example Institution
Identity Management System
Invitation to Tender
Example Institution is convinced of the need for a robust, flexible and extensible Identity Management system. We have an urgent need to replace our existing legacy system for creating and managing user accounts.

We envisage this as a phased project. You are asked to provide:

1. a statement of costs and duration for Phase A;
2. an estimate of the cost and duration of Phase B for our internal planning purposes;
3. a separate quotation for Phase A and estimate for Phase B for linking the system to the institution's student records and personnel systems, comparable to item 1b below;
4. one or more reference sites, with contact names, for an organisation of comparable size where you have built a similar system. An educational establishment is preferred because of the special challenges implied by student registrations and turnover;
5. a brief description of the process you will use to perform Phase A.

PHASE A

1. In consultation with Example Institution's staff, to prepare a detailed specification for a system (or systems):
   i. which will replace and enhance the existing system for creating and managing user accounts and filestore quotas;
   ii. which will automatically create and delete Example Institution staff and student accounts based on the corporate data systems (SRS and HR) and will export mailnames and usernames to those corporate systems;
   iii. that will be extensible to other corporate systems at later stages in the project.
2. In consultation with Example Institution staff, to agree the schema to be supported by the Identity Management system
3. To specify the hardware and software requirements (including numbers of licences) of the above.
4. To provide a statement of costs (software, consultancy, contracting) for delivering and documenting the specified system(s). We will purchase the hardware through our normal channels.
5. To provide a statement of the expected effort required from Institution technical staff.
6. To provide an initial project plan for building the specified systems and migrating existing data.
7. To provide a test and acceptance plan.
8. To specify the options and costs for long-term support and maintenance of the system.

PHASE B

To implement, document and test the system(s) specified in Phase A and migrate existing data.

FURTHER PHASES

These are not yet defined but are likely to involve:

- enable the IdM system to communicate with other corporate database (eg telephone systems);
- deliver information required for authorisation or for application customisation e.g. communities of interest
- implement single-sign-on or synchronised passwords for a variety of applications

BACKGROUND

Example Institution is....
...Scale of institution...
..Details of existing systems...

QUERIES

Any queries or requests for additional information should be addressed to A N Other,
10.5 Conclusions

The procurement and implementation of an IdM system solution - consisting of an amalgam of various related elements that combine together to fulfil the IdM requirements of the academic institution – is a highly important part of any IdM implementation. Choosing a set of products and elements that fit the current needs of the institution and that are flexible enough to meet future needs, and working with vendors that offer the support required, can drastically increase the chances of a successful IdM implementation. Choosing the wrong products and elements can doom such an implementation to failure.

No concrete advice can be given on which IdM products are the “best”, since they all have comparative strengths and weaknesses that can only be understood given a specific set of circumstances. However, following the general advice given in this section, and working in close partnership with vendors and external consultants with a good deal of domain knowledge, can help an academic institution make informed choices as to which set of products and elements making up an IdM system solution is the most suitable for them.
Appendix: Identity Management Glossary

This list is not intended to be exhaustive but contains terms and abbreviations used in IdM, and in other sections of the Toolkit, and their meanings in an IdM context.

API

Abbreviation for "Application Program(ming) Interface". The API for an application defines the methods which other software (possibly including non-local software using the Internet for access) can use to interface with the application, defining conventions and vocabulary for this purpose.

Asset repository

A database in which physical and virtual resources are modelled, used to define and manage access to these resources. Typical resources will include rooms, and the database will define who can enter them, who can book them, etc.

Attribute

A single piece of information about an individual, which may take multiple values. Examples include userID, eduPersonEntitlement, telephone number. Usually aggregated into schemas, particularly in the LDAP context. Attributes are usually stored in a database (sometimes known as a directory), but may also be determined by the user or generated by an identity provider.

Authentication

A process by which an individual proves their identity, particularly electronically. (A common abbreviation for this is AuthN)

Authorisation

The process of determining whether an individual is permitted a level of access to a resource or part of a resource. (A common abbreviation for this is AuthZ)

Certificate

An electronic document which is bound to an entity, such as a server or an individual and can be used to verify their identity. A form of credential.

Credential

Data which can be used to verify the identity of an individual. Common forms of credential include usernames/passwords, certificates, and documents such as passports.

Customisation

The process whereby an individual can determine some of their own attributes rather than using values obtained from other sources such as the institution of which they are a member.

Directory Access Protocol (DAP)

Protocol used to access a directory service. The most popular of these is LDAP.

Directory service

An interface to a database which stores attribute and security information for a number of users. Often used as an Authentication back-end and to supply attributes used for Authorization.

deduRoam (formerly Janet Roaming Service)

Service enabling visitors to participating organisations to use their home network credentials for access (if their home institution is also a member). See http://www.ja.net/services/authentication-and-authorisation/janet-roaming.html. Extends beyond the UK through international partnerships.

Expiry

A built in end date/time to the validity of a credential.

FAM

Abbreviation for "Federated Access Management". Method of providing authenticated access to electronic resources where the authentication is separated from the resource. The authentication system is known as
the "identity provider", and the resource protection system is the "service provider", and access is granted on
the basis of attributes about the user passed from the identity provider to the resource provider.

**Federation**

In Federated Access Management, a federation is a group of service providers and identity providers which
agree to share trust information, and commonly also common standards for attribute usage.

**Identity audit**

Comprehensive investigation into the business processes and technical systems used to manage identity in
an organisation. See detail in audit section.

**Identity management**

Briefly, the processes and systems that allow the creation, retrieval, update, verification and destruction of
identities and information relating to identities including any rights / authority granted to the identities. A fuller
discussion is found in the definition section of the toolkit.

**Identity provider**

In Federated Access Management, the system which handles user authentication and provides attribute
information about the user to the service provider. Usually connects into other systems, such as a directory
service.

**Identity repository**

Database where identity attributes are stored, and tools which allow creation, updating, activation,
suspension, de-duplicating, archiving, deletion and restoration of user accounts. Machines or services may
also have an identity. A fuller discussion is found in the definition section of the toolkit.

**Identity vault**

A directory which contains information central to a variety of other directories, with the aim of managing the
flow of data between directories and improving data quality through deduplication and the reduction of
incompatibility between attributes stored in different directories. Some IDM software uses a relational
database for this instead of a directory.

**KR**

Abbreviation used in this toolkit for "key researcher", the main individual tasked with carrying out an
institutional IdM audit.

**LDAP**

and modifying information in an directory service. See Wikipedia article

**Metadata**

Information describing the properties of an object. In IdM, this is often a person (in which case it would be
"user metadata").

**Password**

A short hidden or encrypted piece of text used to verify the right to a userid for identification of an individual.
Together with the userid, this forms a type of credential.

**Personalisation**

The targeting of service delivery to individuals based on their attributes. (This may include information
provided directly by an individual to the service.) Examples could include highlighting of information deemed
relevant because of departmental membership, or use of a preferred language.

**Portal**

A website which provides access to information stored in a variety of locations. A portal often needs to act as
a proxy to other services, so that users can authenticate to the portal and seamlessly view the information
without further sign on.

**Proxy**
(1) A service which can present credentials to other systems on behalf of logged in users without the users concerned needing to authenticate to these other systems directly. (2) A user who is entitled to perform actions formally restricted to another on their behalf (e.g. as a PA, or to fill in during absence).

**Revocation**
The enforced expiry of a credential, e.g. by the body which issued it in response to loss or misuse.

**SAML**
Security Assertion Markup Language. A standard which describes methods of passing security information online. Used by several FAM applications including Shibboleth to obtain access to resources for users.

**Schema**
Generally a definition of a database structure. In Directory Services, it is the definition of a set of attributes and classes often for a specific purpose. The eduPerson schema, for example, is used to store attributes of students and related objects.

**Service provider**
In FAM, the subsystem responsible for the protection of resources. A service provider should allow access dependent on information provided by a trusted identity provider, and prohibit access when this information is incorrect or absent.

**Shibboleth**
FAM software widely used within the UK Access Management Federation.

**SRS**
Student Record System. Identity repository which is generally the authoritative source of data for students and their interaction with the institution.

**SSO**
Single Sign On. Technology which (in simple terms) allows a user to log on once and thenceforward have access to all the resources to which they are entitled without being challenged for credentials again. In practice, a variety of different levels of SSO are usually available.

**UK Access Management Federation (for Education and Research)**
Organisation of Identity Providers and Service Providers using FAM in the UK.

**userid or username**
A clear text indication of a user's identity, used in partnership with an encrypted or hidden password as a credential.

**Virtual Organisation**
A group of individuals who share common goals and who pool resources, such as a research group or study partners. This definition matches pretty well with Wikipedia's virtual enterprise³⁷.

**WAYF (Where Are You From service)**
FAM component allowing users to choose the Identity Provider which they will use to authenticate to a Service Provider.

---